



Search RISKS using [swish-e](#)

# THE 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 9

**Wednesday 30 May 1990**

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

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

• [Volume 9 Issue 1 \(6 Jul 89\)](#)

- [Elevator inquest update \(Walter Roberson\)](#)
- [UK Defense software standard \(Sean Matthews\)](#)
- [Exxon loses Valdez data \(Steve Smaha -- and Hugh Miller\)](#)
- ["Managing risk in large complex systems" \(Bob Allison\)](#)
- [A "model" software engineering methodology? \(Rich D'Ippolito\)](#)
- [CERT Offline \(Edward DeHart\)](#)
- [Re: Audi 5000 acceleration \(Dave Platt, Mark Seecof, Michael McClary\)](#)

• [Volume 9 Issue 2 \(10 Jul 89\)](#)

- [Re: A "model" software engineering methodology? \(PGN, Stan Shebs, Victor Yodaiken, Dave Davis, Gideon Yuval, Jon Loux\)](#)
- [Re: UK Defence Software Standard \(Eugene Miya, Joshua Levy, Norm Finn\)](#)
- [Exxon file deletions \(Anonymous\)](#)
- [Stalking the wary food shopper \(David Gursky\)](#)

• [Volume 9 Issue 3 \(11 Jul 89\)](#)

- [Re: UK Defense Software Standard \(Nancy Leveson\)](#)
- [Errors in weapon software \(Jon Jacky\)](#)
- [Where does safety lie? \(Jennifer S Turney\)](#)
- [SP Cajon crash \(Mike Trout\)](#)
- [Re: Stalking the wary food shopper \(Steven Den Beste, David Gursky, asente\)](#)
- [ORAI'S'89 Conference Program \(Klaus Brunnstein\)](#)

• [Volume 9 Issue 4 \(13 Jul 89\)](#)

- [Air Traffic Computer Fails 104 Times in a Day \(Rodney Hoffman\)](#)
- [A320/MD-11 F-B-W differ on pilot authority \(Mark Seecof, Rodney Hoffman\)](#)
- [UK MoD S/W Std -- "Crystal Clock" Architecture \(Bob Munck\)](#)
- [A Biological Virus Risk \(Frank Houston\)](#)
- [Software engineering models -- an apology \(Rich D'Ippolito\)](#)

• [Volume 9 Issue 5 \(15 Jul 89\)](#)

- [UK Defence Software Standard \(Dave Parnas, Nancy Leveson, Dave Parnas\)](#)
- [DARPA contract: use AI to select targets during nuclear war \(Jon Jacky\)](#)
- ["Flying the Electric Skies" \(Steve Philipson\)](#)
- [Automobile Electronic Performance management \(Pete Lucas\)](#)

• [Volume 9 Issue 6 \(18 Jul 89\)](#)

- [Mitnick sentenced as an addict \(Rodney Hoffman\)](#)
- [Long addresses confuse bank's computer \(Paul Leyland\)](#)
- [Town Hall's computer snags trouble old age pensioners \(Olivier Crepin-Leblond\)](#)
- [Re: Automobile Electronic Performance Management \(Charles Rader\)](#)
- [Re: UK Defence Software Standard, non-determinism, recursion and armageddon \(Victor Yodaiken, anonymous via Tim Shimeall, Bob Estell, Martin Minow\)](#)
- [Telephone technicians tapping into other phone lines \(Olivier Crepin-Leblond\)](#)
- [Re: New Yorker Article on "radiation" risks \(Gordon Hester\)](#)

• [Volume 9 Issue 7 \(19 Jul 89\)](#)

- [Re: Gordon Hester on Paul Brodeur \(Radiation\) \(Jan Wolitzky\)](#)
- [Computers consume wine \(Hugh Davies\)](#)
- [Mitnick sentence \(Rodney Hoffman\)](#)
- [Re: DARPA contract: use AI to select targets during nuclear war \(Lee Naish\)](#)
- [Reliance on technology \(Jake Livni\)](#)
- [Summer slowdown for RISKS \(PGN\)](#)

• [Volume 9 Issue 8 \(28 Jul 89\)](#)

- [Returning before departing on airline reservation systems \(Gary McClelland\)](#)
- [Sun security problem: restore \(J. Paul Holbrook\)](#)
- [Computer condom? \(Jeff Stout\)](#)
- [Robert Tappan Morris indicted \(Steve Den Beste\)](#)
- [Re: UK Defence Software Standard \(Mark Moraes, Douglas W. Jones\)](#)
- [Polling vs. interrupts \(Douglas W. Jones\)](#)
- [Software Engineering Models \(John \(J.G.\) Mainwaring\)](#)
- [Single Point of Failure for Internet Management \(Kee Hinckley\)](#)
- [DARPA contract & AI for moving targets \(Bob Estell\)](#)
- [Two-Word Last Names and Other Amusing Database Stories \(Gary McClelland\)](#)
- [Credit card issuers invade cardholders' privacy \(Andrew Klossner\)](#)
- [Re: windowless cockpits \(Andrew Klossner\)](#)

• [Volume 9 Issue 9 \(14 Aug 89\)](#)

- [California to escrow electronic vote counting software \(Rodney Hoffman\)](#)
- [Voters Left off Electoral Roll \(Rohan Allan Baxter\)](#)
- [Beeperless remote answering machine risks \(Peter Scott\)](#)
- [Computerized Houses \(Jake Livni\)](#)
- [Automated Driving \(Ian Gent\)](#)
- [Marijuana Virus wreaks havoc in Australian Defence Department \(J. Holley\)](#)
- [Universal Trapdoors \(Vin McLellan\)](#)
- [Computer Problems at Saratoga Racetrack \(Rodney Hoffman, Dave Fiske\)](#)
- [RISKS summer reruns? \(Daniel F. Fisher, Jim Horning\)](#)

• [Volume 9 Issue 10 \(14 Aug 89\)](#)

- [KAL007 - jury finds "willful misconduct" \(Clifford Johnson\)](#)

- [California studies "drive-by-wire" \(Rodney Hoffman\)](#)
- [NY State DMV Computer RISKS \(Will Martin\)](#)
- [RISKS is back in gear \(almost\) \(PGN\)](#)
- ["Radiation" or "Fields" \(Jerry Leichter, Irving Wolfe, John H. Martin, Irving L. Chidsey, Klaus Rieckhoff\)](#)
  
- [Volume 9 Issue 11 \(15 Aug 89\)](#)
  - [Cellular Telephone Causes Airliner Fire Alarm \(Dave Davis\)](#)
  - [Computer-based airline ticket scam \(Rodney Hoffman\)](#)
  - [New Yorker Article on EMF Risks \(Gordon Hester, Dan Schlitt\)](#)
  - [1989 CPSR Annual Meeting \(Gary Chapman\)](#)
  
- [Volume 9 Issue 12 \(17 Aug 89\)](#)
  - [RISKS IS FINALLY MOVING TO CSL.SRI.COM! \(PGN\)](#)
  - [Flaws in calculations, computer models in Trident failures \(Jon Jacky\)](#)
  - [Voyager 2 software faults at launch, 1977 Aug 20 10:29 \(David B. Benson\)](#)
  
- [Volume 9 Issue 13 \(18 Aug 89\)](#)
  - [Phony IRS refunds by computer \(Rob Gross\)](#)
  - [Cellular phones in stings \(David Wittenberg\)](#)
  - [Aircrew acceptance of flight automation \(Robert Dorsett\)](#)
  - [Unauthorized Internet activity \(CERT Internet Advisory -- Kenneth R. van Wyk\)](#)
  - [Re: Marijuana virus wreaks havoc in Australian Defence Department \(Anthony John Apted\)](#)
  - [More on the Wily Hackers \(Rob Gross\)](#)
  - [Training and Software Engineers \(Tim Shimeall\)](#)
  - [Computer-based airline ticket scam \(Jordan Brown\)](#)
  
- [Volume 9 Issue 14 \(21 Aug 1989\)](#)
  - [The Check's in the Mail \(but the water got shut off anyway\) \(Dave Clayton\)](#)
  - [Australian Commonwealth Bank -- doubled deposits \(Martyn Thomas\)](#)
  - [Automatic vehicle navigation systems \(Pete Lucas\)](#)
  - [Tired of computers being trusted? \(a balancing act for wheel watchers\) \(PGN\)](#)
  - [Re: Computer-based airline ticket scam \(Jules d'Entremont\)](#)
  - [Human failures in emergencies \(Henry Spencer\)](#)
  - [Hazards of Airliner Computerization \(Mike Trout\)](#)
  - [Re: California studies "drive-by-wire" \(John Chew\)](#)
  - [First test for electronic tagging starts in jail! \(Olivier Crepin-Leblond\)](#)
  - [Re: unauthorized Internet activity \(anonymous\)](#)
  - [DEMO Software Disk Infected \(Jerusalem Version B\) \(J. Vavrina\)](#)
  
- [Volume 9 Issue 15 \(22 Aug 1989\)](#)
  - [Toronto Stock Exchange down for 3 hours, disk failures \(Peter Roosen-Runge\)](#)
  - [Automated highways ... \(Jerry Leichter, Bill Gorman, Peter Jones, Emily H. Lonsford, Bill Murray\)](#)
  - [Constructive criticism? Technology doesn't have to be bad \(Don Norman\)](#)
  - [Computer Ethics \(Perry Morrison\)](#)
  
- [Volume 9 Issue 16 \(23 Aug 1989\)](#)
  - [Autopilots \(Marc Rotenberg\)](#)
  - [Hazards of Airliner Computerization \(Brinton Cooper\)](#)
  - [Risks, and an assumed definition of "reliability" \(Bob Estell\)](#)
  - [Computers in Medicine \(Brinton Cooper\)](#)
  - [Constructive criticism? Technology doesn't have to be bad \(Donald A Norman\)](#)

- [Tandem computers and stock exchange failure \(Ernest H. Robl\)](#)
- [TSE shutdown -- a success story \(Rich D'Ippolito\)](#)
- [Incompatible IR controllers damage circuits? \(David A Willcox\)](#)
- [Re: a balancing act for wheel watchers \(J. Eric Townsend, Keith D Gregory\)](#)
- [Volume 9 Issue 17 \(23 Aug 1989\)](#)
  - [Hazards in Airliners and Medicine \(Nancy Leveson\)](#)
  - [Re: Technology Doesn't Have to Be Bad \(Mike Trout, Robert Dorsett\)](#)
  - ["Drive-by-wire": What about bicycles? \(Anne Paulson, Donald A Norman\)](#)
  - [Re: Autopilots \(Brinton Cooper\)](#)
  - [Re: Automated Highways \(George H. Feil\)](#)
  - [Roads made safer or not? \(Pete Lucas\)](#)
  - [Training & Software Engineering, a reply... \(Edward A. Ranzenbach\)](#)
- [Volume 9 Issue 18 \(28 Aug 1989\)](#)
  - [Proposal for SDI software center \(Gary Chapman\)](#)
  - [Computerworld article on high-tech weapons \(George Entenman\)](#)
  - [CHAOSNet used in 'SNUFF' snuff \(PGN\)](#)
  - [DMV records, and individual privacy and safety \(PGN\)](#)
  - [Another vehicle guidance system \(Pete Lucas\)](#)
  - [Medics touch computers?!? \(Sam Bassett\)](#)
  - [Unfounded fault-probability claims \(Dieter Muller\)](#)
  - [Lowest-bidder or weak specs? \(David A Honig\)](#)
  - [Automated roads, drive-by-wire, bicycles, and the elderly \(PGN\)](#)
  - [The Guardian vs computer passwords \(Brian Foster\)](#)
- [Volume 9 Issue 19 \(30 Aug 1989\)](#)
  - [NEW INSTRUCTIONS TO FTP VOL i ISSUE j, effective immediately \(PGN\)](#)
  - [Reg. of Motor Vehicles computer slows down \(Adam Gaffin\)](#)
  - [British nuclear reactor software safety disputed \(Jon Jacky\)](#)
  - [South German hackers hack TV German Post \(Klaus Brunnstein\)](#)
  - [Ethics \(Donald J. Weinshank via Tom Thomson\)](#)
  - [sci.aeronautics, a new newsgroup \(Robert Dorsett\)](#)
  - [What's a stamp? \(postal service problems\) \(David Elliott\)](#)
- [Volume 9 Issue 20 \(1 Sep 1989\)](#)
  - [Last Night's "Tonight" was Unknighted; Cars on Carson Top Hat Trick \(PGN\)](#)
  - [More on the Therac 25 -- by Jon Jacky \(PGN\)](#)
  - [Witness questions attack on Iranian jet \(Robert Dorsett\)](#)
  - [Risks of on-line course registration \(Deborah M. Clawson\)](#)
  - [Specifications \(Martyn Thomas\)](#)
  - [Re: Lowest-bidder or weak specs? \(Scott, Robert Hirsch, Bill Cattet\)](#)
  - [Pilot simulator training and boredom \(Dan Franklin\)](#)
  - [More on automation \(Robert Dorsett\)](#)
- [Volume 9 Issue 21 \(5 Sep 1989\)](#)
  - [Re: Technology doesn't have to be bad \(Brian Randell\)](#)
  - [Medical systems and RF interference \(Edward A. Ranzenbach\)](#)
  - ['Business Week' on computers and privacy \(Rodney Hoffman\)](#)
  - [Law == Ethical Consensus \(Scott Guthery\)](#)
  - [US occupational hazards much worse than in Europe, report claims \(Jon Jacky\)](#)

[Are on-line pictures RISKy? \(Russ Nelson\)](#)

- [Non-U.S. Postal Codes -or- Cheap Mail to Europe \(Michael Franz\)](#)
- [Tired of computers being trusted? \(Hugh Davies\)](#)
- [Re: lowest-bidder \(Donald Lindsay, Bill Anderson\)](#)

• [Volume 9 Issue 22 \(6 Sep 1989\)](#)

- [Paris computer takes law into its own hands \(ST4012704 and Sally Jubb\)](#)
- [Brian Randell's comment on fault/failure analysis \(Ted Lee\)](#)
- [Re: US occupational hazards much worse than in Europe \(Mats Ohrman\)](#)
- [Re: medical systems and RF interference \(Brian Kantor\)](#)
- [Re: mis-tagging \(Olivier Crepin-Leblond\)](#)
- [Electronic House Arrest Failure \(Martyn Thomas\)](#)
- [Re: Lowest-bidder or weak specs? \(Henry Spencer\)](#)
- [Re: Law == Ethical Consensus \(Douglas W. Jones, Victor Yodaiken, Gilbert Harman, Eric Hughes, Bill Murray, Joel M. Halpern\)](#)

• [Volume 9 Issue 23 \(12 Sep 1989\)](#)

- [Risks of RISKS: A bug in sendmail and multiple copies of RISKS-9.22 \(PGN, with help from Bill Sommerfeld and Jeff Schiller\)](#)
- [RF susceptibility of electronics \(Pete Lucas\)](#)
- [Some background on the French Farce \(Dave Horsfall\)](#)
- [Organizational Accreditation for Computer Assurance: Some Ideas \(Frank Houston\)](#)

• [Volume 9 Issue 24 \(14 Sep 1989\)](#)

- [RISKS-9.22 and RISKS-9.23 problems had different causes! \(PGN\)](#)
- [Risks of RISKS: A bug in sendmail and RISKS-9.22 \(Scott Mueller\)](#)
- [Phobos 1 & 2 computer failures \(Ralph Hartley\)](#)
- [Aircraft simulators \(Rob Boudrie\)](#)
- [Speeders' Delight? \(Anthony Stone\)](#)
- [Medical accreditation: based on "customer" clout? \(Bob Ayers\)](#)
- [RISKS in mainstream entertainment \(Mission Impossible\) \(Benjamin Ellsworth\)](#)
- [Software Safety Standards \(Anthony J Zawilski\)](#)
- [12th National Computer Security Conference \(Jack Holleran\)](#)

• [Volume 9 Issue 25 \(15 Sep 1989\)](#)

- [Risks of distributed systems \(Eugene Miya\)](#)
- [Medical accreditation: good for big shops only? \(Douglas W. Jones\)](#)
- [The role of government regulation \(Douglas W. Jones\)](#)
- [Is modern software design contributing to societal stupidity? \(Tom Comeau\)](#)
- [Re: Aircraft simulators \(Alan J Rosenthal, Robert Dorsett\)](#)
- [Mission: Impossible \(Robert Dorsett\)](#)

• [Volume 9 Issue 26 \(20 Sep 1989\)](#)

- [Hospital problems due to software bug \(Joe Morris\)](#)
- [Man-Machine Failure at 1989 World Rowing Championships \(Geoffrey Knauth\)](#)
- [Responsibility, Doctors, Military vs Software Developers \(Leslie DeGross\)](#)
- [Organizational Accreditation: More Thoughts \(Frank Houston, Jon Jacky\)](#)
- [An interesting answer to the distributed time problem \(Roy Smith\)](#)
- [Re: Risks of distributed systems \(D. Pardo\)](#)

• [Volume 9 Issue 27 \(21 Sep 1989\)](#)

- [Re: Brian Randell's commentary on safety analysis \(Nancy Leveson\)](#)
  - [Re: Risks of Distributed Systems \(Charles Shub\)](#)
  - [Re: Hospital problems due to software bug \(Will Martin\)](#)
  - [Mailer Bug moves to MCI? \(Jerry Durand\)](#)
  - [Loose wires, master clocks and satellites \(Peter Jones, PGN\)](#)
- [Volume 9 Issue 28 \(24 Sep 1989\)](#)
- [USAir 737-400 crash at LaGuardia \(PGN\)](#)
  - [Re: Hospital problems due to software bug \(Steve VanDevender + Amos Shapir\)](#)
  - [Computers, Planning, and Common Sense \(John \(J.G.\) Mainwaring\)](#)
  - [Synchronizing Clocks \(Earl Boebert\)](#)
  - [Re: Risks of Distributed Systems \(Sung Kwon Chung\)](#)
  - [Master clocks, etc. \(Eddie Caplan\)](#)
  - [ISO 9001 accreditation \(Martyn Thomas\)](#)
  - [Toxic Spill at the Department of Education \[long\] \(Joe Pujals\)](#)
- [Volume 9 Issue 29 \(25 Sep 1989\)](#)
- [Computerized fingerprint system has human failure \(Dave Suess\)](#)
  - [Computerized translation strikes again \(Joe Morris\)](#)
  - [Loose wires \(Desmond Andigo via John Leonard\)](#)
  - [Software \\*IS\\* an abstraction \(Bob Estell\)](#)
  - [Yes, the power grid IS getting less reliable \(Bruce Hamilton\)](#)
  - [Computers, Planning, and Common Sense \(Richard O'Keefe\)](#)
  - [Simulated aircraft emergencies \(John Mackin\)](#)
  - [Re: Software Accreditation \(Richard Threadgill\)](#)
- [Volume 9 Issue 30 \(2 Oct 1989\)](#)
- [The Cuckoo's Egg \(Cliff Stoll\)](#)
  - [Internet cracker on the loose \(Barry Lustig\)](#)
  - [Late night system administration == trouble on SunOS 4.x \(Angela Marie Thomas\)](#)
  - [Date manipulation and end of millennia \(Pete Lucas\)](#)
  - [Re: An interesting answer to the distributed time problem \(Randall Davis\)](#)
  - [Re: Man-Machine Failure at 1989 World Rowing Championships \(Randall Davis\)](#)
- [Volume 9 Issue 31 \(4 Oct 1989\)](#)
- [Computer multiplies taxable earnings by 100 \(Rodney Hoffman\)](#)
  - [Hackwatch spokesman charged \(Dave Horsfall\)](#)
  - [Re: Internet cracker on the loose \(Randy Buckland\)](#)
  - [Re: Hospital problems due to software bug \(Mike Kimura\)](#)
  - [Re: Date manipulation and end of millennia \(Henry Spencer\)](#)
  - [Re: Clock-watching \(George L Sicherman\)](#)
  - [9-digit precision \(Gideon Yuvall\)](#)
  - [The Risks of Crossing the Tracks \(Railroad Crossing Gate Technology\) \(Jean- David Beyer, Laurence Larry Sheldon, Richard L. Piazza via Chuck Weinstock\)](#)
  - [Fifth Annual Computer Security Applications Conference \(Marshall D. Abrams\)](#)
- [Volume 9 Issue 32 \(16 Oct 1989\)](#)
- [Missed zero blamed for air crash \(Dave Horsfall\)](#)
  - [Software reliance/software problems and the Stealth \(Marc Rotenberg\)](#)
  - [Coping with the unexpected - Friday's stock plunge \(Steve Bellovin\)](#)
  - [Re: latest stock market crash \(Olivier Crepin-Leblond\)](#)

[Atlantis launch delay \(PGN\)](#)

- [Keeping up with the \[Indian\(a\)\] Joneses in elections \(PGN\)](#)
- [Friendly advice... \[Datacrime\] \(David Gursky\)](#)
- [Re: Synchronizing Clocks \(Brian Randell\)](#)

• [Volume 9 Issue 33 \(22 Oct 1989\)](#)

- [Earthquake preparedness in computing \(PGN\)](#)
- [Air-Traffic Disruptions \(PGN and Robert Dorsett\)](#)
- [Railroad Level-Crossing Monitoring \(Brian Randell\)](#)
- [Sometimes touch-screens aren't user-friendly \(Jeffrey Mogul\)](#)
- [UK Banking Error \(Brian Randell\)](#)
- [Quotron gores the bears and bares the bulls \(PGN\)](#)
- [Quotron software timing error \(David B. Benson\)](#)
- [Re: latest stock market crash \(David Gursky\)](#)

• [Volume 9 Issue 34 \(24 Oct 1989\)](#)

- [Earthquake and Computers \(Bill Murray\)](#)
- [Black Friday was only grey in Boston \(Pete Kaiser\)](#)
- [Human chess supremacy at risk? \(Bob Barger\)](#)
- [CERT Ultrix 3.0 Advisory \(Ed DeHart\)](#)
- [CERT DECnet Worm Advisory \(Ed DeHart\)](#)

• [Volume 9 Issue 35 \(25 Oct 1989\)](#)

- [Offensive message on electronic information board \(Bob Morris, John Crider\)](#)
- [14-year-old cracks TRW credit for major fraud \(Rodney Hoffman\)](#)
- [Foreplay Doesn't Effect Response Time \(Don Hopkins\)](#)
- ["Computer Virus Countermeasures" Article \(Will Martin\)](#)
- [Hardware failure mimics hackers \(Rob Wright\)](#)

• [Volume 9 Issue 36 \(27 Oct 1989\)](#)

- [Bug in Intel 486 chip \(PGN\)](#)
- [UK Banking Error \(Brian Randell\)](#)
- [The Presentation of Risky Information \(Joshua Levy\)](#)
- [Hardware failure mimics hackers \(Pat White, Andy Goldstein\)](#)
- [Worms in a data stream \(Rick Simkin\)](#)
- [CERT Advisory on Sun RCP \(J. Paul Holbrook\)](#)
- [Warning About CERT Warnings \(anonymous\)](#)
- [Licensed users exceeded \(Tim Steele\)](#)
- [A lesson involving 'CRACKERS' \(APPLE II\) \(Olivier Crepin-Leblond\)](#)

• [Volume 9 Issue 37 \(29 Oct 1989\)](#)

- [Low-tech wins the day in airliner mishap \(Glenn Story\)](#)
- [Hi-tech loses in cars \(Alayne McGregor\)](#)
- [Re: Hardware failure mimics hackers \(Sukumar Rathnam\)](#)
- [Re: Black Friday in Boston and manual systems \(D. W. James\)](#)
- [Re: Human chess supremacy at risk? \(Andrew Klossner\)](#)

• [Volume 9 Issue 38 \(31 Oct 1989\)](#)

- [Passwords in the Electronic Home \(Gary McClelland\)](#)
- [A new excuse \(Ernest H. Robl\)](#)
- [Hot computers and temperature-sensitive programs \(Donald Arseneau\)](#)

- [Re: Hi-tech loses in cars \(Paul Fuqua\)](#)
- [Article on computer crime laws \(Peter Ladkin\)](#)
- [Work processes which are done faster by hand than by machine \(Alexis Rosen\)](#)

• [Volume 9 Issue 39 \(7 Nov 1989\)](#)

- [Computer used to find scoflaws in Boston \(Barry C. Nelson\)](#)
- [Air Traffic in Leesburg VA \(PGN\)](#)
- [Equinox TV Documentary on "Fly By Wire" \(Brian Randell\)](#)
- [Lifethreatening risk! \(related to Soviet PCs\) \(Julian Thomas\)](#)
- [New computer risk: child abuse data base proposed \(W. K. \(Bill\) Gorman\)](#)
- [Dangers of mail aliases \(Jonathan Leech\)](#)
- [Committee report on Bugs \(Bob Morris\)](#)
- [Computer Viruses Attack China \(Yoshio Oyanagi\)](#)
- [First Virus Attack on Macs in Japan \(Yoshio Oyanagi\)](#)
- [NTT Challenges Hackers \(Mark H. W.\)](#)
- [Even COBOL programmers need to know about range checking. \(Bryce Nesbitt\)](#)
- [Unix Expo Power Failure \(Jan I Wolitzky\)](#)

• [Volume 9 Issue 40 \(10 Nov 1989\)](#)

- ["Computer Error" in Durham N.C. election results \(J. Dean Brock, Ronnie W. Smith, John A. Board\)](#)
- [Glitch in Virginia election totals \(Paul Ammann\)](#)
- [Rome: Operator error causes publication of wrong election results \(Lorenzo Strigini\)](#)
- [Delayed Stock Exchange Opening \(Brian M. Clapper\)](#)
- [Electronic Warfare Systems not working--Congress \(\)](#)
- [Computer used to find scoflaws in Boston \(Peter Jones\)](#)
- [Computer errors and computer risks \(Randall Davis\)](#)
- [Equinox program on Airbus \(Lindsay F. Marshall\)](#)

• [Volume 9 Issue 41 \(11 Nov 1989\)](#)

- [Stuffing the electronic ballot box \(again\) \(PGN\)](#)
- [BART and the Bartered-Computer Commuters](#)
- [Coral reef ruined by poor user interface design? \(Jim Helman\)](#)
- [Re: Computer errors and computer risks \(Jerome H Saltzer\)](#)
- [Computer used to find scoflaws in Boston \(David desJardins\)](#)
- [Reference on the early history of Ada -- killing reliably \(Eugene Miya\)](#)

• [Volume 9 Issue 42 \(13 Nov 1989\)](#)

- [Equinox TV programme on A320 \(Bev Littlewood, Chris Dalton\)](#)
- [European Safety is not always BETTER \(Bruce C. Brown\)](#)
- [Artificial lightning \(PGN\)](#)
- [Another intrusive database with associated privacy problems \(Bill Gorman\)](#)
- [Re: "Computer Error" in Durham N.C. election results \(Gregory G. Woodbury\)](#)
- [Re: Computer errors and computer risks \(Willis H. Ware, D. King\)](#)

• [Volume 9 Issue 43 \(15 Nov 1989\)](#)

- [L.A. Times Computer Foulup \(Jerry Hollombe\)](#)
- [Altered bits in Risks 9.39 \(John M. Sullivan and Henk Langeveld\)](#)
- [Re: Apollo 12 \(Artificial lightning\) \(Henry Spencer\)](#)
- [Re: Equinox TV programme on A320 \(Alan Marcum\)](#)
- [Failure of Systems After Earthquake \(Jon von Zelowitz\)](#)
- [Article about "Paperless Office" \(Alan Marcum\)](#)

[Are you sure you declared ALL your dividends? \(Peter Jones\)](#)

- [Re: Another intrusive database ... \(Jim Horning\)](#)
- [Re: Computer errors and computer risks \(David Smith, John Locke\)](#)

• [Volume 9 Issue 44 \(17 Nov 1989\)](#)

- [More on BART's new computer system \(PGN\)](#)
- [Computer misdirects phone calls for TV programme \(Olivier Crepin-Leblond\)](#)
- [Murphy's Law Meets the Navy \(PGN\)](#)
- [Unwanted Credit \(Stuart Bell\)](#)
- [Saskatchewan shuts down translation project \(Peter Jones\)](#)
- [Re: Another intrusive database with associated privacy problems \(Brinton Cooper\)](#)
- [Re: Are you sure you declared ALL your dividends? \(Jim Frost\)](#)
- [Re: L.A. Times "computer" problems \[anonymous\]](#)

• [Volume 9 Issue 45 \(20 Nov 1989\)](#)

- [Another foretaste of the Millenium \(Brian Randell\)](#)
- [UNIX EXPO Blackout \(Brian Randell\)](#)
- [Autodialing horror stories \(John \)](#)
- [Self-trust and computer professionals \(Sean Eric Fagan\)](#)
- [Bit problem with RISKS-9.39 was more global \(Dan Johnson\)](#)
- [Gauge Proposed on Filing of Wage Data by Computer \(David B. Benson\)](#)
- [Congress Finds Bugs in the Software \(David B. Benson\)](#)
- ["Computer risks" \(Randall Davis\)](#)

• [Volume 9 Issue 46 \(22 Nov 1989\)](#)

- ["Play it Again, Yonkers" -- more election funnies \(Steve Bellovin\)](#)
- [Army shuts down computers and goes home due to rain \(Rodney Hoffman\)](#)
- [More good news -- Privacy and risks in credit information \(Bill Gorman\)](#)
- [Automated Bank RISKS \(John Howard Osborn\)](#)
- [Another Foretaste of the Millenium? \(corrigenda\) \(Brian Randell\)](#)
- [Re: Self-trust and computer professionals \(Jerry Hollombe\)](#)
- [Re: Congress Finds Bugs in the Software \(Franklin Davis, Bob, David Gursky\)](#)

• [Volume 9 Issue 47 \(24 Nov 1989\)](#)

- [Air Force Radar Risk \(update\) \(Henry Cox\)](#)
- [Congressional report: "Bugs in the Program" \(Gary Chapman, Dave Davis\)](#)
- [Re: Specifying vs. defining \(Dave Platt\)](#)
- [Training programmers \(Lee S. Ridgway\)](#)
- [Re: Privacy and risks in credit information \(John DeBert\)](#)
- [Re: Automated Bank RISKS \(Marc Shannon, Jon Mauney\)](#)
- [Re: Autodialing horror stories \(Robert Sansom\)](#)

• [Volume 9 Issue 48 \(25 Nov 1989\)](#)

- [Check inquiry / binary search \(anonymous\)](#)
- [Re: Training programmers \(Paul J. Mech\)](#)
- [Telephone Overload \(Jon von Zelowitz\)](#)
- [Write protect tabs \(via Peter Jones from Craig Finseth in VIRUS-L\)](#)
- [High error rates \(P.E.Smee\)](#)
- [Policy vs. the Enabling Technology \(Bill Murray\)](#)
- [Computer Virus Catalog Index: November' 89 \(Klaus Brunnstein\)](#)
- [CERT\\_Tools\\_Announcement \(Edward DeHart\)](#)

• [Volume 9 Issue 49 \(27 Nov 1989\)](#)

- [Davis on arguing about technology vs policy \(Phil Agre\)](#)
- [Re: Check inquiry / binary search: Gardner \(Jim Griffith\)](#)
- [Re: Check inquiry / binary search: Theroux \(Roy Smith\)](#)
- [Re: Privacy and risks in credit information \(Brinton Cooper\)](#)
- [Re: UNIX EXPO Blackout" \(Glenn Story\)](#)
- [How to improve your financial standing \(Glenn Story\)](#)
- [Re: Self-trust and computer professionals \(Mike McNally\)](#)
- [Re: problems with government project specifications \(Bob Estell\)](#)

• [Volume 9 Issue 50 \(3 Dec 1989\)](#)

- [Vote counting problems - experience in Michigan \(Lawrence Kestenbaum, PGN\)](#)
- [Specs and custom software \(Curtis Jackson\)](#)
- [Pentagon Computer Costs \(Gary Chapman\)](#)
- [Software tool munges code \(Nick Lai\)](#)
- [Marshall Williams convicted of destroying data \(PGN\)](#)
- [Mitnick's accomplice sentenced \(Rodney Hoffman\)](#)
- [Desktop forgery \(Rodney Hoffman\)](#)
- [Paul Brodeur's "Currents of Death" \(Werner Uhrig\)](#)
- [McRisks - Electronic Interference in Fast Food Automation \(Robert Horvitz\)](#)

• [Volume 9 Issue 51 \(5 Dec 1989\)](#)

- [Computer bungling of auto insurance premiums \(Barry Kolb\)](#)
- [Computerized voting machine misbehaves \(Rodney Hoffman\)](#)
- [Re: Vote counting problems - experience in Michigan \(Jeffrey R Kell\)](#)
- [Privacy issues raised about automating toll collection \(Stephen W Thompson\)](#)
- [Re: Electronic Interference in Fast Food Automation \(David Chase\)](#)
- [Digital Cellular and the government \(Tim Russell\)](#)

• [Volume 9 Issue 52 \(8 Dec 1989\)](#)

- [Unsafe French software? \(A. N. Walker\)](#)
- [Congress repeals catastrophic insurance, SSA still collects premiums \(Rich Rosenbaum\)](#)
- [Another runaway military computing project: WW/MCCS \(Jon Jacky\)](#)
- [Courts say violation of professional code is malpractice \(Jon Jacky\)](#)
- [Risks of computerized typesetting \(Chuq Von Rospach from SF-LOVERS, via Alayne McGregor\)](#)
- [486 chip faults: PC shipments halted, customers warned \(Jon Jacky\)](#)
- [Selling Government-Held Information \(Peter Jones\)](#)
- [Cellular phone service in Hungary \(Adam J. Kucznetsov\)](#)

• [Volume 9 Issue 53 \(11 Dec 1989\)](#)

- [Computerized public records boon to private eyes probing suitors \(Jay Elinsky, Jon von Zelowitz\)](#)
- [Should computers be legally responsible? \(A. Lester Buck\)](#)
- [Automatic toll systems \(Jerry Harper\)](#)
- [Software Development \(Bill Murray\)](#)
- [Newsgroup posting rejected, rejected, rejected, ... \(Earle Ake\)](#)
- [Comments on Unix INDENT program \(Simson L. Garfinkel, Nick Lai, David McAllister\)\)](#)

• [Volume 9 Issue 54 \(12 Dec 1989\)](#)

- [Mariner I \[once more\] \(Mark Brader and Fred Webb\)](#)
  - [Re: Software tool \(indent\) munges code \(Mark Moraes \[2x\], Joe Dellinger, Amos Shapir\)](#)
-

Re: SSA software maintenance (Dan Franklin)

- [Re: Don't Give Social Security Numbers to Girlfriends \(Will Martin\)](#)

• [Volume 9 Issue 55 \(18 Dec 1989\)](#)

- [Risks of Mail \(the "yellow peril"?\) \(Joe Dellinger\)](#)
- [PR RISKS of computer communications -- Prodigy \(Mark Jackson\)](#)
- [Re: private eyes probing suitors -- Amazon Women on the Moon \(Dwight McKay\)](#)
- [Faults in 29000 RISC chip \(Jon Jacky\)](#)
- [The Trojan horse named "AIDS" \(contributed by many who are not neigh-sayers\)](#)

• [Volume 9 Issue 56 \(21 Dec 1989\)](#)

- [GAO Says IS technology is transforming the Government \(Dave Davis\)](#)
- [California Supreme Court endorses computerized horoscopes \(Clifford Johnson\)](#)
- [Software malpractice \(Steve Philipson\)](#)
- [Computerized card catalog \(Roy Smith\)](#)
- [Frustrated with phones \(Shamus McBride\)](#)
- [23 years MTBF ??? \(David A. Honig\)](#)
- [Re: Another runaway military computing project: WWMCCS \(Tom Reid\)](#)
- [Virus Hearing on TV \(Marc Rotenberg\)](#)
- [Risks of posting to risks! \(Joe Dellinger\)](#)

• [Volume 9 Issue 57 \(4 Jan 1990\)](#)

- [Self-Service ordering in retail establishments \(Russell McFatter\)](#)
- [Programming Languages and Romanian Dictators \(Eric Haines\)](#)
- [`Credit Card' found from 13th Century \(Steve Crocker\)](#)
- [Risks of computerfax \(Steve Elias\)](#)
- [Password Security: A Case History, by Bob Morris and Ken Thompson \(PGN\)](#)
- ["What Really Happened Oct. 13" \(Joe Morris\)](#)
- [The risks of not learning? \(Al Arsenault\)](#)
- [RAND has not received "AIDS Information Disk" \(Correction from Jim Gillogly\)](#)
- [Call for Papers -- 13th National Computer Security Conference \(Jack Holleran\)](#)

• [Volume 9 Issue 58 \(9 Jan 1990\)](#)

- [New-Years' Lotto goes Blotto \(Jim Anderson\)](#)
- [Railroad interlocking systems \(Douglas W. Jones\)](#)
- [Sorry, the bank's already debited your mortgage \(Dave Horsfall\)](#)
- [Positive fingerprint identification? \(Dave Horsfall\)](#)
- [Re: Password Security: A Case History \(Fernando J. Corbato\)](#)
- [The risks of not learning - and of ignoring realities \(Jerry Leichter\)](#)
- [6th Chaos Communication Congress, Hamburg 27-29 Dec 1989 \(Klaus Brunnstein\)](#)

• [Volume 9 Issue 59 \(10 January 1990\)](#)

- [Drawbridge opens without warning in rush-hour traffic \(Jon Jacky\)](#)
- [Massive Electrical Failure in a Bus \(Peter Jones\)](#)
- [What hung the computer? \(Julian\)](#)
- [Passwords and security \(Phil Ritzenthaler, Henry Spencer, Jerry Leichter, ark, Peter da Silva\)](#)
- [IEEE Symposium on Research in Security and Privacy, Oakland 1990 \( \)](#)

• [Volume 9 Issue 60 \(15 Jan 1990\)](#)

- [The C3 legacy: top-down goes belly-up recursively \(Les Earnest\)](#)
- [Dispatchinate Computerized Cab Service \(PGN\)](#)

- [Risks of manual page formatters and inserted text \(J. Eric Townsend\)](#)
- [Re: What hung the computer? \(Dave Platt\)](#)
- [Perils of not planning for errors \(Ted Shapin\)](#)
- [Wrong 800 numbers \(Steven W. Grabhorn\)](#)
- [Password Sharing \(Dave Bafumo\)](#)
- [Call for papers for computer security foundations workshop \(John McLean\)](#)

• [Volume 9 Issue 61 \(20 Jan 1990\)](#)

- [Shortage of RISKS but no shortage of risks -- the week in review \(PGN\)](#)
- [AT&T Failure \(Bill Murray, Jim Horning\)](#)
- [Risks of Voicemail systems that expect a human at the other end \(R. Aminzade\)](#)
- [Risks of vote counting \(Alayne McGregor\)](#)
- [Risks of supermarket checkout scanners \(David Marks\)](#)
- [European R&D in Road Transportation \(Brian Randell\)](#)
- [Old habits die hard \(Dave Horsfall\)](#)

• [Volume 9 Issue 62 \(26 Jan 1990\)](#)

- [Australian medical database linkages \(Michael Bednarek\)](#)
- [Cause of AT&T network failure \("Telephony", Jim Harkins\)](#)
- [London Stock Market Disruption \(courtesy of Steve Milunovic\)](#)
- [Railway interlocking \(Clive Feather\)](#)
- [More risks to computers \(Richard Thomsen\)](#)
- [Re: Risks of supermarket checkout scanners \(Marvin Moskowitz, Doug Renner, Don Craig\)](#)
- [Robert T. Morris Convicted \(Michael J. Chinni\)](#)
- [Advance Program for Oakland Symposium \(REVISED\) \(Debbie Cooper\)](#)

• [Volume 9 Issue 63 \(31 Jan 1990\)](#)

- [Vive la difference? \(Peter G. Neumann\)](#)
- [Airbus crash of June 88 \(Olivier Crepin-Leblond\)](#)
- [AT&T Crash Statement: The Official Report \(Don H Kemp via Geoff Goodfellow\)](#)
- [Important Lesson from AT&T Tragedy \(Bill Murray\)](#)
- [Potential Lesson From AT&T \(Bill Murray\)](#)
- [Sun Sendmail Vulnerability \(Kenneth R. van Wyk\)](#)
- [GPO Library disk infection \(PC\) \(Kenneth R. van Wyk\)](#)
- [Re: Password Sharing \(Al Arsenault\)](#)
- [Annual Computer Security Applications Conference \(Marshall D. Abrams\)](#)
- [Virology \(Gene Spafford\)](#)

• [Volume 9 Issue 64 \(1 Feb 1990\)](#)

- [SENDMAIL horrors \(PGN\)](#)
- [Software error at Bruce nuclear station \(Mark Bartelt\)](#)
- [New South Wales Police deregisters police cars \(Diomidis Spinellis\)](#)
- [Fire and 753 controllers \(need a light?\) \(Neal Immega via Mark Seiden\)](#)
- [The substantiative error made by AT&T \(Robert Ullmann\)](#)
- [Re: AT&T Crash Statement: The Official Report \(Bob Munck\)](#)
- [Re: Airbus crash of June 88 \(Robert Dorsett\)](#)
- [Re: Virology and an infectious date syndrome \(Gene Spafford\)](#)

• [Volume 9 Issue 65 \(2 Feb 1990\)](#)

- [The C3 legacy, Part 2: a SAGE beginning \(Les Earnest\)](#)
- [Sendmail Flaw \(Geoffrey H. Cooper\)](#)

[Filing 1040 Electronically \(Bill Murray\)](#)

- [Predicting Problems \(David desJardins\)](#)
- [Airbus crash \(Dave Morton\)](#)
- [The Trojan horse named 'AIDS' revisited \(PGN\)](#)

• [Volume 9 Issue 66 \(5 Feb 1990\)](#)

- [Another SAGE memoir \(Jon Jacky\)](#)
- [DoD plans another attack on the "software crisis" \(Jon Jacky\)](#)
- [The Cultural Dimensions of Educational Computing \(Phil Agre\)](#)
- [Vincennes' Aegis System: Why did RISKS ignore specifications? \(R. Horn\)](#)
- [Computer Virus Book of Records \(Simson L. Garfinkel\)](#)
- [Re: AT&T \(Gene Spafford, David Keppel, Stanley Chow\)](#)
- [Sendmail \(Brian Kantor, Rayan Zachariassen, Geoffrey H. Cooper, Kyle Jones, Craig Everhart\)](#)
- [Re: Risks of Voicemail systems \(Randall Davis\)](#)

• [Volume 9 Issue 67 \(8 Feb 1990\)](#)

- [Shoplifting and Computers \(Curtis P. Yeske\)](#)
- [New movie Script writer \(Olivier Crepin-Leblond\)](#)
- [Re: Computers, good and evil \(George L Sicherman\)](#)
- [The C3 legacy, Part 3: Command-control catches on \(Les Earnest\)](#)
- [Vincennes' ROEs revisited \(Clifford Johnson\)](#)
- [SOGS - Hubble Space Telescope software now ready \(Rodney Hoffman\)](#)
- [AT&T and reentrant code \(John A. Pershing Jr\)](#)
- [AT&T and error recovery \(Jonathan I. Kamens\)](#)
- [Dillard's Dept Stores Use SSN as Sales ID - Printed on Receipts \(Allen Gwinn\)](#)
- [AutoAlarms \(Robert J Woodhead\)](#)

• [Volume 9 Issue 68 \(14 Feb 1990\)](#)

- [Re: Caller ID \(NYTimes editorial\) \(John M. Sullivan\)](#)
- [How to make answering machines deliver ransom messages \(Denis Coskun\)](#)
- [More on the Hubble Space Telescope \(Hank Strub\)](#)
- [Human blamed, not the computer! -- jury duty \(Lee S. Ridgway\)](#)
- [Accents are more than just decorations \(Kai-Mikael J{{-Aro\)](#)
- [\[Parse-ly, Rosemary, Time, Light, Control & Other SAGE Remarks\] \(Martin Minow\)](#)
- [Blazers \(Jeff Berkowitz\)](#)
- [Re: Computers, good and evil \(Gregg TeHennepe\)](#)
- [Telephone Switch Security \(Roland Ouellette\)](#)

• [Volume 9 Issue 69 \(20 Feb 1990\)](#)

- [A320 accident \(Nancy Leveson, George Michaelson\)](#)
- [Ferry line replaces "sail-by-wire" with pneumatic controls \(Jon Jacky\)](#)
- [Now Prodigy Can Read You \(Donald B Wechsler\)](#)
- [3 KGB Wily Hackers convicted, mild sentences \(Klaus Brunnstein\)](#)
- [Problems/risks due to programming language, stories requested. \[Item Includes AT&T "do...while"..."switch"..."if"..."break" tale\] \(Gerald Baumgartner\)](#)
- [AT&T Says New Goof Wiped Out Many Toll-Free Calls \(David B. Benson\)](#)
- [Re: Computerized Collect Calls \(Adam Gaffin via Mark Brader\)](#)
- [RISKS of ANI blocking \(James C Blasius\)](#)
- ["Brilliant Pebbles" \(Gary Chapman\)](#)

• [Volume 9 Issue 70 \(23 Feb 1990\)](#)

[Neutron reactor lands in hot water \(Steve Strassmann\)](#)

- [Yet another laserwriter health risk? \(Roy Smith via Mark Seiden\)](#)
- [Computer security at stock exchanges vulnerable \(Rodney Hoffman\)](#)
- [A320 accident \(Udo Voges\)](#)
- [Problems/risks due to programming language \(AT&T Bug\) \(Jonathan I. Kamens, Steve Nuchia, David L. Golber, Robert L. Smith\)](#)
- [Re: "Provably insecure programming language" \(Mark McWiggins\)](#)
- [Re: Computerized Collect Calls \(Joseph Beckman\)](#)
- [What makes a hacker hack? \(Nigel Voss-Roberts\)](#)
- [The "Twelve Tricks" Trojan horse \(Christoph Fischer via John Rushby\)](#)

• [Volume 9 Issue 71 \(26 Feb 1990\)](#)

- [Journalists and computers: `Z' \(R. Clayton\)](#)
- [Space Shuttle \(Steve Bellovin\)](#)
- [Magellan spacecraft will need frequent guidance from Earth \(David B. Benson\)](#)
- [More on Air India Airbus A320 \(Steve Milunovic\)](#)
- [AT&T \(Clifford Johnson, Rob Warnock, Steve Bellovin, David Paul Hoyt\)](#)
- [Re: Computerized Collect Calls \(John \(J.G.\) Mainwaring\)](#)
- [A different multiple-copy problem \(SEN\) \(Dan Craigen\)](#)

• [Volume 9 Issue 72 \(28 Feb 1990\)](#)

- [Clients cross about crossed wires \(David Sherman\)](#)
- [100-year-old can drive four years without test \(David Sherman\)](#)
- [Some comments on the Airbus \(Robert Dorsett, Martyn Thomas\)](#)
- [Re: Problems/risks due to programming language \(Bruce Hamilton\)](#)
- [Comments on programmer error \(Geoffrey Welsh\)](#)
- ["Goto considered harmful" considered harmful \(Brad Templeton\)](#)
- [lockd \(Caveh Jalali\)](#)
- [Re: Railroad interlocking systems \(J.A.Hunter via Brian Randell\)](#)

• [Volume 9 Issue 73 \(6 Mar 1990\)](#)

- [Another 100-year computer saga \(David B. Benson\)](#)
- [Traffic System Failure \(Rich Neitzel\)](#)
- [Railway interlocking systems \(Clive Feather\)](#)
- [Avionics in the media \(John M. Sullivan\)](#)
- [Re: A320 \(Steven Philipson, Subhasish Mazumdar, Pete Mellor\)](#)
- [Mileage Plus wants me to move \(Tim Kay\)](#)
- [Credit-card fraud \(Douglas Mason\)](#)

• [Volume 9 Issue 74 \(12 Mar 1990\)](#)

- [Airbus Crash: Reports from the Indian Press \(N. Balaji\)](#)
- [Indian Airlines A320 in the German press \(Udo Voges\)](#)
- [The C3 legacy, Part 4: A gaggle of L-systems \(Les Earnest\)](#)
- [The risks of keeping old versions -- Daigle book \(Graeme Hirst/David Sherman\)](#)
- [PSU Hackers thwarted \(Angela Marie Thomas\)](#)
- [Anonymous Word Processing: `Z' \(Jon von Zelowitz\)](#)
- [Re: Now Prodigy Can Read You \(Eric Roskos\)](#)
- [Re: Traffic System Failure \(Peter Ahrens\)](#)
- [Tracking criminals and the DRUG police-action \(J. Eric Townsend\)](#)
- [Human-Centered Automation \(Robert Dorsett\)](#)
- [Drive-by-wire cars \(Craig Leres\)](#)

• [Volume 9 Issue 75 \(15 Mar 1990\)](#)

- [PRODIGY updating programs \(Simson L. Garfinkel\)](#)
- [Who shall guard the guards? \(Robert A. Levene\)](#)
- [Journalistic hacking \(Rodney Hoffman\)](#)
- [Caller-id by name \(Gary T. Marx\)](#)
- [Re: PSU Hackers thwarted \(David C Lawrence\)](#)
- [Re: Tracking criminals and the DRUG police-action \(Brinton Cooper\)](#)
- [RISKS of "Evolutionary Software" \(Rajnish and Gene Spafford via Will Martin\)](#)
- [Human-centered automation \(Donald A Norman\)](#)
- [Re: Airbus Crash: Reports from the Indian Press \(Henry Spencer\)](#)

• [Volume 9 Issue 76 \(19 Mar 1990\)](#)

- [How history gets made, or, myths spread like viruses at the CVIA \(Doug McIlroy\)](#)
- [London Underground wrong-way train in rush-hour \(Brian Randell\)](#)
- [Privacy in Printout \(L. P. Levine\)](#)
- [Send it by FedEx = Don't Send It At All! \(Betsy Perry\)](#)
- [20th Int. Symp. on Fault-Tolerant Computing \(Neil Speirs\)](#)

• [Volume 9 Issue 77 \(21 Mar 1990\)](#)

- [Stranded Satellite \(Steve Bellovin\)](#)
- [Re: London Underground wrong-way train in rush-hour \(Richard A. Schumacher\)](#)
- [Internet Intruder \(John Markoff via PGN \(excerpted\)\)](#)
- [Internet Intruder Warning \(J. Paul Holbrook\)](#)
- [Risks of reporting breakins \(Randal Schwartz\)](#)
- [Re: Privacy in Printout \(Tim Wood, Henry Spencer\)](#)
- [Computer-based phones threaten privacy \(again!\) \("34AEJ7D"\)](#)

• [Volume 9 Issue 78 \(5 Apr 1990\)](#)

- [RAF Tornado collision \(Dorothy R. Graham via PGN\)](#)
- [New Georgia Automobile Tags \(Warren Tucker\)](#)
- [British tax tales \(Bob Gray via Mark Brader\)](#)
- [Oslo Day in Norway? No way! \(Paul Dorey\)](#)
- [Computer backorder on cover letters \(Yuri Rubinsky\)](#)
- [London Underground driver's action \(Martyn Ould\)](#)
- [Hi-Tech Loo \(Wayne W. Lui via Brian Randell\)](#)
- [Proposed UK Authority for Risk Management \(Brian Randell\) \[See Box for cases\]](#)
- [More on Prodigy's Updating of a User's Disks \(Eric Roskos, Paul Eggert\)](#)
- [April Fools Day on the net \(D. Waitzman via Martin Minow\)](#)
- [Automated Fast Food \(Dave Curry\)](#)
- [UNIX Trix \(Paul Eggert\)](#)
- [Re: PSU Hackers thwarted \(Pete Mellor\)](#)
- [Three Australians indicted for computer tampering \(PGN\)](#)

• [Volume 9 Issue 79 \(9 Apr 1990\)](#)

- [Fixing Computer Error Cost \\$1,300 in Overtime \(Chris McDonald\)](#)
- [Computer problem delays Calif. Lotto payouts \(Rodney Hoffman\)](#)
- [Computer Glitch Cuts of Decco Sales \(Mark Adams\)](#)
- [Computer Animations in court testimony \(Peter Scott\)](#)
- [Re: Proposed UK Authority for Risk Management \(Dan Franklin\)](#)
- [Re: Intruders arrested \(Mike McBain via Lee Naish\)](#)
- [Re: More on Prodigy's Updating of a User's Disks \(Leonard Erickson\)](#)

- [Wonderfully mistaken letter generators \(Frank Letts, Gary Cattarin\)](#)
- [Re: Automated Fast Food \(Webber\)](#)
- [Re: Airbus Crash: Reports from the Indian Press \(Dan Brahme\)](#)
- [A320 press excerpts \(Robert Dorsett\)](#)
- [Indian A320 crash \(Henry Spencer\)](#)
- [The two A320 crashes show similarities \(Martyn Thomas\)](#)
  
- [Volume 9 Issue 80 \(13 Apr 1990\)](#)
  - [Risks of Daylight Savings Time \(Chuck Weinstock\)](#)
  - [Authentication via User-Defined Fields \(Jim Kimble\)](#)
  - [Rites of consumption \(Phil Agre\)](#)
  - [Franklin Resources Computer Glitch \(John Murray\)](#)
  - [Risks of computerized publishing \(Henry Spencer\)](#)
  - [Re: Computer generated letters \(Benjamin Ellsworth, Nathaniel Borenstein\)](#)
  - [Software: A320 vs. shuttle \(Michael\)](#)
  - [The C3 legacy, Part 5: Subsystem I \(Les Earnest\)](#)
  - [COMPASS 90 program and registration information \(John Cherniavsky\)](#)
  
- [Volume 9 Issue 81 \(18 Apr 1990\)](#)
  - [RISKS, SENDMAIL, and YOU! \(PGN\)](#)
  - [London Tube train leaves ... without its driver \(Stephen Page\)](#)
  - [Shuttle roll incident on January '90 mission \(Henry Spencer\)](#)
  - [Software failures on Boeing 747-400? \(Trevor Warwick\)](#)
  - [False 1099 forms \(Phil R. Karn\)](#)
  - [Re: Risks \[9.080\] of Daylight Savings Time \(Thomas Zmudzinski, Chuck Weinstock\)](#)
  - [Comment on UK Software Standards \(Richard Morton\) \[RISKS-9.1 and 2\]](#)
  - [Automates Fast Food \(David Bank\)](#)
  
- [Volume 9 Issue 82 \(20 Apr 1990\)](#)
  - [A320 news \(Henry Spencer\)](#)
  - [The Danger of Airbags \(Jeff Deifik\)](#)
  - [Re: Risks of computerized publishing \(Paolo Mattiangeli\)](#)
  - [Postal Employees and cross-matching \(Brinton Cooper\)](#)
  - ["It's a Computer Error" \(Lindsay F. Marshall\)](#)
  - [Re: London Tube Train \(Clive Feather\)](#)
  - [London Underground Low-Tech \(anonymous\)](#)
  - [Virus outbreak in China! \(R.Gowans via MCGDRKG in Virus-L\)](#)
  
- [Volume 9 Issue 83 \(25 Apr 1990\)](#)
  - [You think YOU have problems with your telephone company? \(PGN\)](#)
  - [Traffic light outages \(King Ables\)](#)
  - [Sabbath Goes High-Tech \(David Dabney\)](#)
  - [Computers and Hyphenated names \(Allan Meers\)](#)
  - [London tube train and the Boeing 747 ... \(Clive Walmsley\)](#)
  - [Risky McDonald's comrade... \(David Gursky\)](#)
  - [Risks of engine computers and EMP \(Lynn R Grant\)](#)
  
- [Volume 9 Issue 84 \(26 Apr 1990\)](#)
  - [Re: You think YOU have problems with your telephone company? \(Gary Chapman, David G. Novick, Vincent, Laura Halliday, Al Stangenberger, Pete McVay, John Higdon, Greeny\)](#)
  
- [Volume 9 Issue 85 \(27 Apr 1990\)](#)

- [Computer error parks hundreds illegally \(Dave Harding\)](#)
- [Computers may be fattening? \(Gary Tom\)](#)
- [Unattended Plane Take-off \(Andrew Duane\)](#)
- [Aircraft electronics problems: A pilot's report \(Peter Ilieve\)](#)
- [1099 forms, risks, and technology \(Gregg TeHennepe\)](#)
- [Re: "It's a Computer Error" \(Pete Mellor\)](#)
- [Re: Risks of engine computers and EMP \(David Paul Hoyt\)](#)
- [Security Breach--cc:Mail Inc. \(Chris McDonald\)](#)
- [Queues and Servers \(Anthony E. Siegman\)](#)
- [Computers and names with special characters \(Lance Hoffman\)](#)
- [Computer Jammimg of 911 LInes \(Gary McClelland\)](#)

• [Volume 9 Issue 86 \(30 April 1990\)](#)

- [Futures market shut down \(Steve Bellovin\)](#)
- [Habsheim A320 crash \(Clive Feather\)](#)
- [Throttle Hitch Hits 747-400 \(Robert Dorsett\)](#)
- [Re: Unattended Plane Take-off \(Jan I Wolitzky\)](#)
- [Re: Computers and names with special characters \(Mike Van Pelt\)](#)
- [Inadequate documentation - truncated GPAs \(Doug Sewell\)](#)
- ["The return of the hacker" \(David B. Benson\)](#)
- [Indian Professors Teaching Virus Writing \(Cliff Stoll\)](#)
- [\(Not necessarily\) computer parks hundreds of cars illegally \(Bill Gunshannon\)](#)

• [Volume 9 Issue 87 \(1 May 1990\)](#)

- [Phones & techologically illiterate operators \(David A. Honig\)](#)
- [More telephone problems -- union pressures \(Peter Jones\)](#)
- [Forwarding: Weird phone bills - an unexplored possibility \(Chaz Heritage via Richard Busch\)](#)
- [Re: Call Forwarding \(Peter Jones\)](#)
- [Kissimmee Kate \(Geoffrey H. Cooper\)](#)
- [Re: You think YOU have problems with your telephone company? \(Gary Cattarin, Jozsef A Toth, Warren Levy\)](#)
- [Blaming it on the computer? \(Brad Templeton\)](#)
- [Re: Risky McDonald's comrade... \(Charles Youman\)](#)

• [Volume 9 Issue 88 \(2 May 1990\)](#)

- [Booby-trapped contracted software \(Tom Kopp\)](#)
- [Death rate inflated in St. Bruno area, health report finds \(David Sherman\)](#)
- [Software Bug Causes Shuttle Countdown Hold at T-31 Seconds \(Karl Lehenbauer\)](#)
- [Criticism of "Glass Cockpits" \(1\) and \(2\) \(Martyn Thomas\)](#)
- [A320 Bangalore crash \(Martyn Thomas\)](#)
- [A320 criticisms reported \(Martyn Thomas\)](#)
- [Re: computer parks hundreds of cars illegally \(Andrew E. Birner\)](#)
- [\(Apparently\) widespread problem with census 800 number \(Timothy M. Wright\)](#)
- [Re: You think YOU have problems with your telephone company? \(Chris Lewis\)](#)
- [Telephone switch problems \(Webber\)](#)
- [White paper available: "Improving the Security of Your UNIX System" \(Davy Curry\)](#)
- [Virus found in a game software on the market \(Yoshio Oyanagi\)](#)
- [Re: Computers and names with special characters \(Bandy\)](#)

• [Volume 9 Issue 89 \(7 May 1990\)](#)

- [A funny thing happened at the lottery office \(Alan Hargreaves\)](#)

- ['Boy, 12, allegedly taps credit files' \(Ira Greenberg\)](#)
- [Robert T. Morris' sentencing \(PGN\)](#)
- [Hazards Of Office Laser Printers \(Keith Dancy\)](#)
- [Re: Aircraft electronics problems PIREP \(Steve Jay, Robert Dorsett\)](#)
- [Re: A320 criticisms reported \(Robert Dorsett\)](#)
- [Phone system problems \(Gail L Barlich, Steve Bellovin, Andras\)](#)
- [Phone Switch Resets \(Avi Belinsky\)](#)
- [Other ways to get "Improving the Security of Your UNIX System" \(Davy Curry\)](#)
- [So many weapons, so little radio spectrum \(Chug Von Rospach\)](#)
- [Und der Hyphisch \(Andy Behrens\)](#)

• [Volume 9 Issue 90 \(10 May 1990\)](#)

- [The Mayor and the EMail \(John Markoff\)](#)
- [Democratic bug in AppleLink! \(Hector Rojas\)](#)
- ['Hacker' alters phone services \(David G. Novick\)](#)
- [Re: A funny thing happened at the lottery office \(Mike Beede, Emmett Hogan\)](#)
- [Risk of Unauthorized Access to TRW Credit Database \(Larry Lippman\)](#)
- [Unusual traffic light behaviour \(Andy Coombes\)](#)
- [High School Boy's Story was a Fake \(Yoshio Oyanagi\)](#)
- [More about Sharp's Viri in Japan \(Yoshio Oyanagi\)](#)
- [ARMY wants computer viruses for battlefield use \(Gary McClelland\)](#)
- [A-320 avionics malfunctions \(Vic Riley\)](#)

• [Volume 9 Issue 91 \(13 May 1990\)](#)

- [Hubble Telescope pointing in the wrong direction \(Raymond Chen\)](#)
- ["Feds Pull Plug On Hackers" \(James K. Huggins\)](#)
- [Airline booking cancellation \(Pete Mellor\)](#)
- [Simple tone dialler bypasses British Telecom charging \(Nigel Roberts\)](#)
- [Risks of caller identification \(David A. Honig\)](#)
- [Avoiding ANI by Dialing 1-900 \(Gary McClelland\)](#)
- [Duplicate Mailings of RISKS 9.89 -- BITNET \(Emmett Hogan\)](#)
- [Re: Hazards of laser printers \(Paul DuBois, Peter Jones\)](#)
- [IFIP Conference Call for Papers \(Rick Schlichting\)](#)
- [CALL FOR PAPERS: Computing and Ethics \(Donald Gotterbarn\)](#)

• [Volume 9 Issue 92 \(17 May 1990\)](#)

- [Army chafes under Congress' robot weapons ban \(Jon Jacky\)](#)
- [Re: \[London\] Tube train leaves ... without its driver \(Gavin Oddy\)](#)
- [Re: First Hubble Images Delayed To Conduct Focusing Tests \(Karl Lehenbauer\)](#)
- [ANI for the criminal as well as the private citizen \(Brad Templeton\)](#)
- [Computer Virus Solicitation \(Andy Warinner\)](#)
- [Feds Pull Plug On Hackers \(Bob Sutterfield, Rick Clark\)](#)
- [Re: Military Viruses \(Jim Vavrina via David Brierley\)](#)
- [Re: Magnetic ID cards for all Israeli citizens \(Amos Shapir\)](#)
- [Risks of Laser Printouts \(David Tarabar\)](#)

• [Volume 9 Issue 93 \(21 May 1990\)](#)

- [Stamford CT 18-hour telephone switch outage affects 27,000 lines \(PGN\)](#)
- [Irrational and nonvaledictory reasoning \(PGN\)](#)
- [Crackdown on 1-900-STOPPER? \(John M. Sulak\)](#)
- [P.T.U.U.I. \(Robert Hardy, PGN\)](#)
- [Military Computer Virus Contract \(Rory J. O'Connor\)](#)

- [Risks of Laser Printouts \(Simson L. Garfinkel\)](#)
- [Directions and Implications of Advanced Computing, DIAC-90 \(Rodney Hoffman\)](#)

• [Volume 9 Issue 94 \(25 May 1990\)](#)

- [More on Stamford CT Telephone Switch Outage \(PGN\)](#)
- [Duplicate RISKS mailings...SOLVED! \(Emmett Hogan\)](#)
- [Cross about CRIS \(Crime Report information System\) \(Pete Mellor\)](#)
- [Disk failures after extended shutdown \(David Keppel\)](#)
- [The Internet is growing up! \(Scott Deerwester\)](#)
- [Are government secrets safer if not classified? \(Mary Culnan\)](#)
- [Risks of slandering ... in public forums \[re: P.T.U.U.I.\] \(Tom Blinn\)](#)
- [A320 again \(Nancy Leveson\)](#)
- [M1 Air Crash Inquest \(Brian Randell\)](#)
- [Tempus Fugit -- Claremont Clock Tower Tick Talk \(Brian Randell\)](#)
- [Telephone network synchronization and NavSat \(John T. Mulqueen via James Price Salsman via JC%RMC\)](#)
- [National Geographic also wants me to move \(Tim Kay\)](#)
- [Re: Irrational and nonvaedictory reasoning \(John Chew\)](#)

• [Volume 9 Issue 95 \(26 May 1990\)](#)

- [Possible Anti-Virus Legislation \(Robert Smithmidford via Thomas Zmudzinski via Linda K. Perez\)](#)
- [Secure UNIX Infected? \(Craig Harmer via Russ Davis via Linda K. Perez\)](#)
- [Follow-up on Fed Raids on Hackers \(David Ruderman\)](#)
- [Crypto '90 conference, 11-15 August 1990, UC Santa Barbara \(John Gilmore\)](#)

• [Volume 9 Issue 96 \(29 May 1990\)](#)

- [Roller Coaster Accident Blamed on Computer \(Gary Wright\)](#)
- [ATMs robbed with no signs of tampering \(Stephen W Thompson\)](#)
- [Bank deposits huge amount in account and blames owner! \(Richard Muirden\)](#)
- [Risks in secure documents \(David Fuller\)](#)
- [You Think YOU Have Trouble with Your Telephone Company? \(Donald B. Wechsler\)](#)
- [Steve Jackson Games & A.B. 3280 \(Brian Sherwood\)](#)
- [Re: Secure UNIX Infected? \(Steve Bellovin, Henry Spencer\)](#)
- [Dereferencing Tim Kay's address \(David Kuder\)](#)

• [Volume 9 Issue 97 \(30 May 1990\)](#)

- [The C3 Legacy, Part 6: Feedback \(Les Earnest\)](#)
- [Re: You Think YOU Have Trouble with Your Telephone Company? \(Rodney Hoffman\)](#)
- [Right to Privacy, Public Funds, and the 2600 \(Bob Estell\)](#)
- [Re: Steve Jackson Games & A.B. 3280 \(Chuq Von Rosbach\)](#)
- [Re: ATMs robbed with no signs of tampering \(Bob Campbell\)](#)
- [Re: ATMs robbed in Trump Castle \(Avi Belinsky\)](#)
- [Re: Secure UNIX Infected? \(Mark Gabriele\)](#)



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 9: Issue 1

Thursday 6 July 1989

## Contents

- [Elevator inquest update](#)  
[Walter Roberson](#)
- [UK Defense software standard](#)  
[Sean Matthews](#)
- [Exxon loses Valdez data](#)  
[Steve Smaha -- and Hugh Miller](#)
- ["Managing risk in large complex systems"](#)  
[Bob Allison](#)
- [A "model" software engineering methodology?](#)  
[Rich D'Ippolito](#)
- [CERT Offline](#)  
[Edward DeHart](#)
- [Re: Audi 5000 acceleration](#)  
[Dave Platt](#)  
[Mark Seecof](#)  
[Michael McClary](#)
- [Info on RISKS \(comp.risks\)](#)

---

### Elevator inquest update

<Walter\_Roberson@CARLETON.CA>

Fri, 30 Jun 89 11:07:29 EST

Another two days of the testimony into the April 1st elevator fatality in Ottawa has revealed some interesting/ scary facts.

It seems that the elevator type in question had a known problem with potentially being able to move when only one of the two doors was closed. A repair which involved moving only \*one\* wire was known, and had been recommended by the manufacturer in 1978. The repair was not made until 4 days \*after\* the accident, 11 years later.

In the meantime, the ownership of the building changed hands (in 1980), and the maintenance company changed (in 1988). The government inspectors never noticed that the change hadn't been made (there are only 2 inspectors for the Ottawa area, which has 3000+ elevators), and the

new repair company didn't notice it either. The owner of the company that checked the elevator just 1 hour before the death \*was\* aware of the change notice, but, as he put it:

"Are you telling me 10 years after a letter comes out... I should remember that?" [...]

"I would assume in 1980 [when the building was sold -- WDR] all those changes would be made, let alone 1988 [when he took over maintenance]. I don't know of any way any elevator company could know about it all."

The scary part came at the end of yesterday's article:

"The inquest was told no maintenance records were available for the elevators, installed with building construction in 1973. Records are not required by the ministry and are often removed by maintenance companies if the contract expires in order to hinder the new contractors, Allan Maheral said."

[The Ottawa Citizen, 28 June 1989, p. B1, and 29 June 1989, pp. A1-A2]

Walter Roberson <Walter\_Roberson@Carleton.CA>

---

## **UK Defense software standard**

*Sean Matthews <sean@aipna.edinburgh.ac.uk>*

*Fri, 30 Jun 89 13:49:12 BST*

I have just seen a copy of the UK department of defence draft standard for safety critical software (00-55).

Here are a few high (and low) points.

1. There should be no dynamic memory allocation (This rules out explicit recursion - though a bounded stack is allowed).
2. There should be no interrupts except for a regular clock interrupt.
3. There should not be any distributed processing (i.e. only a single processor).
4. There should not be any multiprocessing.
5. NO ASSEMBLER.
6. All code should be at least rigourously checked using mathematical methods.
7. Any formally verified code should have the proof submitted as well, in machine readable form, so that an independent check can be performed.
8. All code will be formally specified.
9. There are very strict requirements for static analysis (no unreachable

code, no unused variables, no uninitialised variables etc.).

10. No optimising compilers will be used.

11. A language with a formally defined syntax and a well defined semantics, or a suitable subset thereof will be used.

Comments.

1. means that all storage can be statically allocated. In fact somewhere it says that this should be the case.

2-4 seem to leave no option but polling. This is impractical, especially in embedded systems. No one is going to build a fly by wire system with those sorts of restrictions. (maybe people should therefore not build fly by wire systems, but that is another matter that has been discussed at length here already). it also ignores the fact that there are proof methods for dealing with distributed systems.

5. This is interesting, I seem to remember reading somewhere that Nasa used to have the opposite rule: no high level languages, since they actually read the delivered binary to check that the software did what it was supposed to do.

6-7. All through the draft the phrase 'mathematical methods' or 'formal methods' is \*invoked\* in a general way without going into very much detail about what is involved. I am not sure that the people who wrote the report were sure (Could someone from Praxis - which I believe consulted on drawing it up - enlarge on this?).

8. this is an excellent thing, though it does not say what sort of language should be used. Is a description in terms of a Turing machine suitable? After all that is a well understood formal system.

10. Interestingly, there is no requirement that the compiler be formally verified, just that it should conform to international standards (though strictly), and not have any gross hacks (i.e. optimisation) installed. There is also no demand that the target processor hardware be verified (though such a device exists here already: the Royal Signals Research Establishment's Viper processor).

11. seems to be a dig at Ada and the no subsets rule. It also rules out C.

Conclusions.

I find the idea of the wholesale mayhem and killing merchants being forced to try so much harder to ensure that their products maim and kill only the people they are supposed to maim and kill, rather amusing.

The standard seems to be naive in its expectations of what can be achieved at the moment with formal methods (That is apparently the general opinion around here, and there is a \*lot\* of active research in program verification in Edinburgh), and impossibly restrictive.

An interesting move in the right direction but too fast and too soon. And they might blow the idea of Formal verification by trying to force it too soon. And I would very much like to see these ideas trickle down into the civil sector.

I might follow this up with a larger (and more coherent) description if there is interest (this was typed from memory after seeing it yesterday) there is quite a bit more in it.

Sean Matthews

Dept. of Artificial Intelligence JANET: sean@uk.ac.ed.aipna

University of Edinburgh ARPA: sean%uk.ac.ed.aipna@nsfnet-relay.ac.uk

80 South Bridge UUCP: ...!mcvax!ukc!aipna!sean

Edinburgh, EH1 1HN, Scotland

---

### **Exxon loses Valdez data**

*Steve Smaha <Smaha@DOCKMASTER.NCSC.MIL>*

*Wed, 5 Jul 89 11:58 EDT*

This appeared in the 2 Jul 89 Austin (TX) "American-Statesman".

"Exxon accidentally destroys data files on Alaska oil spill,"

by Roberto Suro, New York Times Service

HOUSTON - A computer operator at Exxon headquarters in Houston says he inadvertently destroyed computer copies of thousands of documents with potentially important information on the Alaskan oil spill.

A federal court had ordered Exxon to preserve the computer records along with all other material concerning the grounding of the Exxon Valdez in Prince William Sound on March 24 and the subsequent cleanup effort.

Les Rogers, a spokesman for the Exxon Company USA, confirmed the destruction of the computer records but said the oil company's lawyers believed other copies exist.

"Very early in the spill, even before the court order, Exxon took the initiative to instruct all its employees to save all documents relating to the event because of the anticipated litigation," Rogers said. "We assume these instructions have been followed."

The computer technician, Kenneth Davis, said that it would be difficult and perhaps impossible to determine what documents were on destroyed computer files.

Exxon faces about 150 lawsuits as a result of the spill, which dumped 11 million gallons of crude oil into Prince William Sound, and it appears certain that the loss of these documents will be the subject of court arguments.

Stephen Sussman, a Houston lawyer involved in a suit against Exxon on behalf of Alaska fishermen, Native Americans, and others, said, "The destruction of these records is potentially significant to our case in that we will be arguing that Exxon has been negligent throughout this disaster and now perhaps it was negligent even in the handling of its own documents."

Davis, 33, was dismissed June 8, the day after the destruction of the

records was discovered.

In several interviews, and in written statements to the Texas Employment Commission, Davis alleged that his superiors had been negligent in safeguarding the computer records and that his actions resulted from their failures.

The destroyed material included all internal communications and word-processing documents from both the Exxon Shipping Co., which owned the tanker, and the executive offices of Exxon USA.

Davis said that since the tapes were the only complete copy of what passed through those computer systems, it might be impossible to determine what was lost.

[The full NYT text was sent in by Hugh Miller <MILLER@vm.epas.utoronto.ca>, who prefaced the text with this reference to '1984' by George Orwell:

``I was thinking just this morning about how Winston Smith's job in historical engineering would have been a lot easier if everything had been kept on magnetic media, when this item appeared in today's NYT."`

To conclude, he made some comments about the difficulties of prosecuting after the documents have been destroyed (with reference to Ollie and Fawn).  
``Want to bet Exxon doesn't use a PROFS system?''

---

### ✂ IEEE Spectrum June issue: "Managing risk in large complex systems"

<bobal@microsoft.UUCP>  
Wed Jul 5 16:40:22 1989

The June 1989 issue of IEEE Spectrum contains a series of articles discussing risk management techniques and failures, paying particular attention to the areas of aging aircraft ala the Aloha Airlines 737 incident, the Hinsdale fire which shut down phone service near Chicago, the Savannah river nuclear reactors, the space shuttle, and the release of lethal chemicals in Bhopal.

Perhaps because of my own particular biases, the space shuttle article was particularly interesting where it describes the risk of a shuttle accident also dooming the space station (due to the destruction of single copies of critical space station components).

Bob Allison

---

### ✂ A "model" software engineering methodology? ([RISKS-8.86](#))

<rsd@SEI.CMU.EDU>  
Mon, 03 Jul 89 14:46:23 EDT

In [RISKS 8.86](#), Jon Jacky quotes Stan Shebs:

We supposedly had a "model" software engineering methodology; what I remember most clearly is that half the work was done on one flavor of IBM OS, and the other half done on a different flavor, and file transfer

between the two was tricky and time-consuming.

The coupled clauses are unrelated, a compositional practice Mr. Shebs is apparently quite fond of. Let's concentrate on Mr. Sheb's text to see what his understanding of software development is:

The day-to-day work was [...] writing the "Program Design" for an already-written program (is that stupid or what), figuring out how to compute the intersection of two polygons in space.

Without context, this is not evidence that the SE method was good or bad. Of course the program design should have been documented beforehand, but recognizing that it is necessary to have for testing and maintenance purposes is not stupid. I have seen many systems where the software is very old (or inherited) and must be re-documented to current standards. What was the case here?

I suppose the greatest risk of failure derives from things that weren't anticipated during testing, such as a Siberian snowdrift changing the topography on a navigation map...

[How does the snow get on the map?!] One does not wait until testing to anticipate such contingencies. Does Mr. Shebs think so?

(Regarding) statistics on software quality, the closest thing we had was maybe a count of problem reports (hundreds, but each report ranged from one-liners to one-monthers in terms of effort required).

Sigh. There is no mention here whether this applies to delivered product or corrected production errors. Is this his view of what constitutes quality?

Nothing classified, we had the odd situation that the *\*data\** was [sic] classified, but the *\*program\** wasn't even rated "confidential"!

Odd situation? Apparently, Mr. Shebs had a single experience in the MCCR community.

This article was posted to illuminate "the accuracy/quality of strategic weapons guidance systems", presumably by offering a coherent and reasoned exposition. Instead, it presents jokes, innuendo, and unsubstantiated charges and conclusions in indefinite (and sloppy, such as the 1/2 inch diameter missile) language such as:

The difficulty of all this apparently didn't occur to anybody until after the missile was working...

...error accumulation over 2000 km is immense,...

...cute little cassette tapes...

The precision and formality of the software was very low, but it was exhaustively tested over and over and over again.

Really, if Mr. Shebs's rambling demonstrates anything, it shows that the greatest risk is hiring inarticulate and confused programmers like himself who don't have the faintest idea what software engineering is.

Mr. Shebs appears to come clean in only one statement:

The fragility of something like the cruise missile and its software is something I've spent a lot of time wondering about, and don't really have any idea.

Indeed.

Rich D'Ippolito

---

### **🚨 CERT Offline [Computer Emergency Response Team]**

*<Edward DeHart <ecd@cert.sei.cmu.edu> [forwarded via many different paths]>  
Wed, 5 Jul 89 14:19:09 EDT*

The supply of cold water to our air-conditioners has been turned off due to a major break in the pipes. The problem may not be corrected until the weekend.

The lack of cold water is bad news for the computer room. All of the systems are going to be turned off.

For the next day or so, CERT will not be able to send or receive EMAIL via the Internet.

We will be in the building if you need to contact us. Our telephone number is 412-268-7090.

Please forward this information to others in your group.

Thanks, Ed DeHart

[whhaha yuh know; CERT needs a CERT! The police dept's computers are down ... Willis Ware]

[I suppose the famous detective, Air-Cool Pour-out, will investigate. PGN]

---

### **🚨 Re: Audi 5000 acceleration [[RISKS-8.87](#)]**

*Dave Platt <dplatt@coherent.com>  
Fri, 30 Jun 89 10:40:37 PDT*

- > The study, "An Examination of Sudden Acceleration," explored ...
- >
- > However, there was evidence of minor surges of about three-tenths of the
- > Earth's gravity for 2 seconds caused by electronic faults in the idle
- > stabilizer systems of the Audi 5000 ... the surge could startle a driver
- > enough to accidentally push the accelerator instead of the brake, ...

Minor?? .3G works out to roughly 10 feet/sec<sup>2</sup>, or a zero-to-sixty acceleration time of about 9 seconds. This may not be considered "full power" or "major" acceleration for a sports-car, but my old Volvo has difficulty reaching highway speed (55) in 9 seconds even if I floor the accelerator.

A .3G surge for 2 seconds would accelerate a car from a standstill to somewhere in the neighborhood of 20 feet/second, and would carry the car about 10 feet forwards. Startling? I should say so... especially to drivers who might have only recently switched to the Audi from an older, lower-powered car.

Even if this fault in the idle stabilizer cannot invoke "full" acceleration by itself, it sounds substantially dangerous in and of itself. Coupled with poor pedal/linkage layout and design, it apparently adds up to a real hazard.

Dave Platt FIDONET: Dave Platt on 1:204/444 VOICE: (415) 493-8805  
USMAIL: Coherent Thought Inc. 3350 West Bayshore #205 Palo Alto CA 94303

---

### ***#* misleading Audi surge report**

*<icc.marks@SEAS.UCLA.EDU>*

*Fri, 30 Jun 89 11:39:11 PDT*

Three-tenths of the Earth's gravity is not "minor." That's about three meters per second squared. At the end of two seconds the car would have travelled about six meters or twenty feet. 3m/sec<sup>2</sup> on a 1500 Kg automobile for just a moment will set it moving fast enough to squish or bash-in any likely obstacle (inertia, you know).

I'll bet drivers are startled! They aren't likely to accelerate that fast when parking... Sixty miles per hour is about a hundred kilometers per hour. That's about twenty-eight meters per second. At 3m/sec<sup>2</sup> it takes only nine or ten seconds to reach 28m/sec; the owners of Audi 5000's are probably pleased with the "zero to sixty in six seconds" performance of their cars; that's less than 5m/sec<sup>2</sup>. (Many cars can't do 0-60 in less than 9 seconds flat out.) This means the "surges... caused by electronic faults" are equivalent to accelerating away from a stop light in traffic--and only a third less than flooring the gas pedal to get onto the Pasadena Freeway in Highland Park. Imagine if you were easing your car into your garage at an idle and it suddenly accelerated like you were taking off from a stop sign.

(Before you all write to criticize the math, I'm aware that I've neglected air resistance and gear shifting, but I don't think this invalidates the

discussion.)

If the report does minimize the fault in the Audi's electronic controls to lay the blame on the driver, then we must ask whether the authors wanted to shift concern away from Audi where it seems to belong. (No, I've never owned or even driven an Audi.)

Mark Seecof, Locus Computing Corp., Los Angeles (213-337-5218)  
My opinions only, of course...

---

✂ **Audi surges (Re: [RISKS DIGEST 8.87](#))**

Michael McClary <michael@xanadu.COM>  
6 Jul 89 18:06:27 GMT

>However, there was evidence of minor surges of about three-tenths of the  
>Earth's gravity for 2 seconds caused by electronic faults in the idle  
>stabilizer systems of the Audi 5000

Is this a missprint? I find the characterization of a two-second, 3/10 g surge as "minor" to be ludicrous.

This is especially true if it is the result of a malfunction in an idle speed control system, implying that it would occur when the vehicle was stopped. At a busy intersection, for instance, with pedestrian cross-traffic or another stopped car just a foot or two ahead.

After one second, a 3/10g surge would have moved the vehicle almost five feet forward, and have it traveling over 6 1/2 MPH. By the end of the two second surge, if nothing is done, the car would be doing 13 MPH and have gone nearly twenty feet.

No hypothetical "pedal misapplication" is necessary to make such a vehicle hazardous, and while zero-to-sixty in under ten seconds may not be full throttle for an Audi, it's close enough for me.



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 9: Issue 2

Monday 10 July 1989

## Contents

• [Re: A "model" software engineering methodology?](#)

[PGN](#)

[Stan Shebs](#)

[Victor Yodaiken](#)

[Dave Davis](#)

[Gideon Yuval](#)

[Jon Loux](#)

• [Re: UK Defence Software Standard](#)

[Eugene Miya](#)

[Joshua Levy](#)

[Norm Finn](#)

• [Exxon file deletions](#)

[Anonymous](#)

• [Stalking the wary food shopper](#)

[David Gursky](#)

• [Info on RISKS \(comp.risks\)](#)

---

✉ **Re: A "model" software engineering methodology? ([RISKS-8.86](#))**

*Peter G. Neumann <Neumann@KL.SRI.COM>*

*Mon, 10 Jul 89 09:01:23 PDT*

I apologize to Stan Shebs and to RISKS readers for not having sufficiently exerted my responsibility as moderator regarding the Shebs/D'Ippolito exchange. Sorry. Occasionally one slips by. Rich D'Ippolito's message was less than circumspect. I probably should have let them try to agree on a counterposition and a rebuttal before troubling you all. However, there are some important issues raised.

A response from Stan Shebs follows, along with four other commentaries.

---

✉ **Re: A "model" software engineering methodology? ([RISKS-8.86](#))**

Stan Shebs <[shebs@apple.com](mailto:shebs@apple.com)>

Fri, 7 Jul 89 12:02:57 PDT

I didn't expect such a violent reaction to my comments on cruise missile software that appeared in [RISKS-8.86](#), but several of my remarks really ought to be clarified. First off, I worked on ALCM 1981-82, fresh out of Texas A&M, with no programming experience outside of research projects, and my only education in software engineering having been to read "The Mythical Man-Month". Boeing did not require any training in their software methodology (they probably offered some, but I don't remember), we just learned on-the-job. (Friends who are still there tell me that things have improved in the past several years.) My original article was written as personal impressions, for a non-expert audience, and unfortunately Jon's quoting couldn't make it into more of a learned treatise.

> From: [rsd@SEI.CMU.EDU](mailto:rsd@SEI.CMU.EDU)

> In [RISKS 8.86](#), Jon Jacky quotes Stan Shebs:

<> We supposedly had a "model" software engineering methodology; what I  
<> remember most clearly is that half the work was done on one flavor of IBM  
<> OS, and the other half done on a different flavor, and file transfer  
<> between the two was tricky and time-consuming.

> The coupled clauses are unrelated, a compositional practice Mr. Shebs is  
> apparently quite fond of.

In this case, it was a subtle (clearly too subtle) literary device; there was almost no relation between the official methodology and daily practice. The process of conforming to the DoD's requirements resulted in a fanatical adherence to the letter of the standards, with almost no concern for actual quality. I had written some tricky code and proved its correctness; it got thrown away because it was "too general". We had an independent auditor that checked over the documentation and found missing commas, while completely ignoring the parts of the program design that parroted Fortran code without saying anything about its structure. I could go on, but this is supposed to be a clarification, not an independent message.

> [...]

> Of course the program design should have been documented beforehand, but  
> recognizing that it is necessary to have for testing and maintenance  
> purposes is not stupid. I have seen many systems where the software is very  
> old (or inherited) and must be re-documented to current standards. What was  
> the case here?

The software was about a year old I believe; probably the same standards were in effect then, but I can't say for sure. It was written under considerable time pressure and almost entirely free of comments. The experience of trying to puzzle out the workings of 30k lines of mixed Fortran, Cobol, and assembler was truly horrible. Management knew it was all a sham, but they just asked us to go along with it. (Funny, 30k lines doesn't seem like a lot anymore - times change...)

<> (Regarding) statistics on software quality, the closest thing we had was

<> maybe a count of problem reports (hundreds, but each report ranged from  
<> one-liners to one-monthers in terms of effort required).

> Sigh. There is no mention here whether this applies to \_delivered\_ product  
> or corrected production errors. Is this his view of what constitutes  
> quality?

I believe the numbering of software problem reports started after delivery of the first version, but I don't know for sure. The whole setup seemed pretty disorganized; for instance, there was no formal system for module-level testing, before or after delivery, and regression testing was limited to rerunning a set of standard flight paths, which weren't complicated enough even to test all the paths in the program code, let alone boundary cases.

> This article was posted to illuminate "the accuracy/quality of strategic  
> weapons guidance systems", presumably by offering a coherent and reasoned  
> exposition. Instead, it presents jokes, innuendo, and unsubstantiated  
> charges and conclusions in indefinite (and sloppy, such as the 1/2 inch  
> diameter missile) language such as:

It never occurred to me that anybody could possibly misinterpret "6 meters long and 1/2 in diameter", but it must be possible. For the record, it's 1/2 \*meter\* (actually more like 2/3, but who cares).

<> The difficulty of all this apparently didn't occur to anybody until after  
<> the missile was working...

This was what I heard from the people who were there at the time. They may not have been entirely accurate, but the objective evidence and the history of the ALCM program support this. Old documents seem to assume that laying out a mission by hand in the traditional way is good enough. In actuality, the missile is so sluggish that it has to begin climbing long before it reaches a hill, or it will end up plowing into the side (this actually happened during testing).

<> ...error accumulation over 2000 km is immense,...

We had graphs of just how bad inertial navigation gets over long distances. The actual numbers are probably classified, but in general an inertially guided missile would be useful only against cities; silos and other hardened sites require much more accurate navigation techniques.

> Rich D'Ippolito

stan shebs                      shebs@apple.com

---

### **✶ Ad hominem arguments and "model" s.e. methodology**

*victor yodaiken <yodaiken%ccs2@cs.umass.edu>  
Fri, 7 Jul 89 01:55:27 EDT*

I found the comments of Rich D'Ippolito in [RISKS 9.1](#) ("A 'model' software

engineering methodology") to be unconvincing and ill mannered. Mr. D'Ippolito is offended by a some anecdotes posted in [RISKS 8.86](#) which reflect poorly on the design and implementation of a cruise missile ( John Jacky, quoting Stan Shebs). The points which Mr. D'Ippolito references are:

- 1) The development was carried out on 2 incompatible development platforms --- file transfer between the 2 systems was ``tricky and time consuming".
- 2) The "Program Design" was written after the program was written.
- 3) There failure conditions of the program seemed to have been poorly planned for, e.g, error accumulation over a long flight path, and the effects of snowfall on topography.
- 4) Program quality was measured by raw count of problem reports without reference to the complexity of the reported problems.

These are all significant problems, which cannot be dismissed by the ad hominem arguments presented by Mr. D'Ippolito. Mr. Shebs is not the first person to point out instances of sloppy software engineering in D.O.D. projects, but I found his story interesting and informative. Mr. D'Ippolito argues in the mode of a press secretary, rather than as a scientist. Comments such as:

>Really, if Mr. Shebs's rambling demonstrates anything, it shows that the  
>greatest risk is hiring inarticulate and confused programmers like himself  
>who don't have the faintest idea what software engineering is.

are out of place and offensive.

Victor Yodaiken

---

## **✉ Shebs/D'Ippolito**

*Dave Davis <davis@community-chest.mitre.org>  
Fri, 07 Jul 89 08:16:47 -0400*

In the 6 July Risks Mr. D'Ippolito somewhat justifiably takes Mr. Shebs to task about his criticisms of the Cruise Missile project Mr. Shebs was a part of.

However, one comment relating to producing the design specification after coding was completed brought back my memories of being one of the senior staff during the mid-80s for the Navy's version of this missile, called Tomahawk.

In the view of the project's mangement, the required documentation was an unnecessary burden placed on us hardworking developers by government bureaucrats. An example was the spec. which provided an English description fo the guidance software line-by-line. It was essentially useless. The guidance software had been developed in the usual atmosphere of intense deadline pressure, with the highest priority given to making the thing work. As a result, the code was not a textbook example of modularity and understandability. In fact, the documentation probably was irrelevant, since the engineers and computer scientists used simulations of the guidance system and software models of the guidance equations to develop the system.

My point is that these projects are examples of the fact that industry is just beginning to recognize the size of the investment they are making in software, and the technologies needed. Most defense contractors (there is a Carnegie-Mellon survey on this) are only now coming out of the Stone Age of focusing on coding in marathon sessions to produce software while producing reams of documentation.

However, it is by no means clear that applying what we think of as state-of-the-art that we will do much better.

---

### **✶ personalities**

*Gideon Yuval 1.1114 x4941 <gideony@Microsoft.UUCP>*

*Fri Jul 7 11:20:34 PDT 1989*

I think a large part of the comments by [rsd@sei.cmu.edu](mailto:rsd@sei.cmu.edu), in the 6/Jul/89 Risks-digest, were personal attacks on Stan Shebs; such attacks are relevant to risks only to the extent that they discourage whistle-blowers, lest the ayatollahs attack them too. Was that the intention of these remarks?

Gideon Yuval, [gideony@microsoft.com](mailto:gideony@microsoft.com), 206-882-8080 (fax:206-883-8101;TWX:160520)  
Paper-mail: Microsoft, 16011 NE 36th way, Redmond, Wa., 98073-9717

---

### **✶ Re: A "Model" Software Engineering Methodology?**

*Jon Loux <JLOUX@UCONNV.M.BITNET>*

*Fri, 7 Jul 1989 09:52:25 EST*

In [RISKS Digest 9.1](#) a certain gentleman responds and quotes liberally from another gentleman's experiences in software engineering for missile guidance systems. The jist of the article seemed to be that the original poster was incompetent and that his remarks were irrelevant, derogatory, and totally without merit. Ahem, Isn't this just possibly another example of shooting the messenger because of the message???

I once worked for a defense contractor who manufactured submarines for the U.S. Navy (There are only two in this country, take your pick.) Quite often there was a tremendous difference between The Way It Is and The Way It Is Supposed To Be. Sometimes design and manufacturing errors were found. Sometimes they were buried. But usually, the reputation (of the company and the Navy) was more important than the viability of the product.

The RISKS involved are probably as old as engineering itself; that is, creating an absurd or impossible situation, and then deriding the first person who brings attention to the problem. Where would the Emperor be today if someone had not pointed out the 'design flaw' in his new clothes?

If we cannot learn from our mistakes, we just rename them; "Success". (1/2 :-)

Jon Loux

The University of Connecticut

Flames? Go ahead, bake my Cray.

---

**✉ Re: UK Defence Software Standard ([RISKS-9.1](#))**

*Eugene Miya <eugene@eos.arc.nasa.gov>*

*Fri, 7 Jul 89 11:15:27 PDT*

Sean Mathews brings back shades of when I was working on flight projects. Dicey stuff. All examples he documents (starting with no dynamic memory [I was amused by starting with this]) are all standard operating procedure (so believed in the defense and aerospace arenas). These ideas date back decades (not just years). Since NASA was mentioned (and projects differ), I should mention that the policy of explicitly reading machine code is from the days of smaller memories. The Agency is trying to get away from this. The code is still generated (I know where this example comes from) by HAL/S computers for the shuttle (HAL, BTW does not have dynamic memory, or any of the features [no multiprocessor support, etc.]).

Sean's posting does raise quite a few other questions:

- Is there explicit range checking?
- Are there comments on performance?
- Are there specifications on clocks and interrupt handling?
- Etc.

For the classic summary to Sean's misgivings of the merchants of killing and mayhem. It was Andy Mickel at U. Minn. who in the early days of Ada published: "Reliable software must kill people reliably." [Pascal News].

--eugene miya

---

**✉ Re: UK Defence Software Standard ([RISKS-9.1](#))**

*Flame Bait <hplabs!joshua@Atherton.COM>*

*Fri, 7 Jul 89 13:41:14 PDT*

Here are some comments on Sean Matthews's posting:

>1. There should be no dynamic memory allocation (This rules out explicit >recursion - though a bounded stack is allowed).

As a practical matter, this requirement rules out all real software systems. Also, I do not see why this makes software safer. I think this will result in less safe software, since there will be arbitrary limits on the length of everything. All last names must be 30 chars or less, all place names must be 40 chars or less, etc. Long buffer sizes will lessen the impact, but take up more space.

>2. There should be no interrupts except for a regular clock interrupt.

>3. There should not be any distributed processing

>4. There should not be any multiprocessing.

As a practical matter, these requirements rule out most (all?) real systems. Also, I do not see why software which does none of these things is safer than software which does all of them. These requirements seems to be designed to compensate for the (huge) limitations of current program verification techniques.

>10. No optimising compilers will be used.

What is an optimising compiler? This is a serious question. GCC with no arguments provides better code than PCC or Sun's CC, does that make it an optimized compiler? What if you give it a -O1 option, or a -O3 option (which turns on more optimization). All compilers do some optimization. Point 10 should say something like "All compilers used must be verified to the same level of certainty as the programs they are compiling." It is kind of useless to verify a program and then run it through a compiler which is not verified. Of course writing a compiler which does not use dynamic memory (see point 1) would be an interesting exercise!

Overall, I found these standards funny, not useful. My conclusion is that no safety critical software can not be written in the UK since points 1 and 2 will mean that none of it will be up to standard.

Joshua Levy joshua@atherton.com work:(408)734-9822 home:(415)968-3718

---

### **✂ Re: UK Defense software standard**

*Norm Finn <ultra!norm@ames.arc.nasa.gov>*

*Thu, 6 Jul 89 19:01:05 PDT*

Sean Matthews writes of the UK safety-critical software standard:

> 2-4 seem to leave no option but polling. This is impractical,  
> especially in embedded systems. No one is going to build a fly by  
> wire system with those sorts of restrictions.

Polling is absolutely the safest and most-used method for programming embedded systems for safety-critical applications. It is a commonly held fallacy that the essence of a real-time embedded system is FAST response to external stimuli -- that interrupts are therefore important. The essence of real-time embedded systems is a GUARANTEE of a specified, finite response time to EACH stimulus.

Many embedded systems divide real time into a hierarchy of time slots, and execute fixed subroutines in each time slot (i.e. "polling"). This makes it relatively easy to verify that the program can meet all response time requirements. Stimuli requiring slower responses are handled by routines that run less often, and routines running more often handle stimuli requiring faster response. Every routine can be proven to run in less time than the length of one time slot.

Additional advantages: The trivial scheduling algorithm makes the interaction between the routines vastly easier to write and verify than is the case in a

system that can switch tasks at random times. Response time bottlenecks can be identified and addressed early in the development cycle. It is easy to match the requirements of the sources/sinks of stimuli/responses and the capabilities of the embedded computer. And on and on ...

In short, when a life depends on your system ...

KISS (Keep It Simple [,|and] Stupid)

Norm Finn

Ultra Network Technologies, 101 Daggett Dr., San Jose, CA 95134 (408) 922-0100

---

### **✂ Exxon file deletions**

<[Anonymous]>

*Fri, 7 Jul 89 09:45:56 PDT*

While the previous posting in RISKS didn't mention this, the "destroyed files" regarding the Exxon oil spill were apparently actually simply the routine recycling of a month-old (or older) backup dump tape.

Exxon has continued to state that they believe all files are still online or in paper form. Obviously the correct procedure would have been to explicitly order the preservation of those dumps, and nobody wants to condone Exxon's handling of this whole affair, but it is worth noting that the deletion in question was apparently the result of routine computer center operations common to many environments, not some "explicit" act of destruction.

---

### **✂ Stalking the wary food shopper**

*David Gursky <dmg@lid.mitre.org>*

*Sun, 9 Jul 89 13:36:14 EDT*

Today's (09 July 89) Washington Post has several articles about the latest trend in foods: Frequent Shoppers Programs. For those of you not aware of this, it is similar to Frequent Flyer Programs used by the airlines. When you buy an item at your local mega-chain supermarket, your purchase is noted in a large customer database and you are given a credit on your account, and when your account reaches certain defined levels, you receive coupons for various foodstuffs. Simple right? Wrong.

First, the markets are proposing to record more than a purchase of so many dollars and cents. They intend to record the specific brands and items you bought. Based on this information and your address information, markets want to start targetting mailings of flyers and coupons to you. If their records show you have started to buy baby food recently, the AI routines that examine the data base will note this, and flag your record to be sent coupons on other baby products, such as diapers and lotions.

This is in fact not a terrible thing. If markets want to spend money send paper in the mail to people who may or may not use them, there are far more useless ways to spend money. The problem is the second application.

It seems that the markets want to sell this information to the manufacturers (the Campbell Soups, the Nabiscos, the General Foods, and so on) for use by their own marketing people. This also raises the traditional right to privacy issues.

I wonder how much longer it will be till I will not be able to go into my local Giant Food and buy a bag of flour, because their demographic survey shows that no one eats in my apartment building.



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 9: Issue 3

Tuesday 11 July 1989

## Contents

- [Re: UK Defense Software Standard](#)  
[Nancy Leveson](#)
- [Errors in weapon software](#)  
[Jon Jacky](#)
- [Where does safety lie?](#)  
[Jennifer S Turney](#)
- [SP Cajon crash](#)  
[Mike Trout](#)
- [Re: Stalking the wary food shopper](#)  
[Steven Den Beste](#)  
[David Gursky](#)  
[asente](#)
- [ORAI89 Conference Program](#)  
[Klaus Brunnstein](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✉ Re: UK Defense Software Standard (by Joshua Levy, [RISKS-9.2](#))

Nancy Leveson <nancy@ICS.UCI.EDU>

Mon, 10 Jul 89 22:39:04 -0700

Joshua Levy comments in [Risks 9.2](#) on the UK MoD Std:

- <>1. There should be no dynamic memory allocation (This rules out explicit  
<> recursion - though a bounded stack is allowed).
- <>2. There should be no interrupts except for a regular clock interrupt.
- <>3. There should not be any distributed processing
- <>4. There should not be any multiprocessing.

>As a practical matter, these requirements rule out most (all?) real systems.  
>Also, I do not see why software which does none of these things is safer than  
>software which does all of them. These requirements seems to be designed to  
>compensate for the (huge) limitations of current program verification  
>techniques.

Much safety-critical software is built this way already; it is simply untrue that these limitations rule out real systems. Software with these characteristics is safer because it is deterministic rather than non-deterministic -- the number of states may often be reduced to a small enough number to perform extensive (and sometimes exhaustive) testing and analysis. No dynamic storage allocation also ensures that the system will not run out of memory during a critical operation: Again the goal is to make the software predictable and analyzable. Norm Finn, in the same issue of Risks, explains the reasons for and practicality of eliminating interrupts.

Safety-critical systems are built this way in order to perform effective verification (e.g., testing and analysis) in general -- it has nothing to do with the limitations of formal verification. I refer you to the design of the software for a nuclear reactor shutdown system described in my Computing Surveys article (June 1986) as an example and an explanation of the purpose of such restrictions.

>Of course writing a compiler which does not use dynamic memory (see point 1)  
>would be an interesting exercise!

You misunderstood -- the limitation is on the object code, not on the compiler. If the compiler runs out of memory and fails to produce object code, this is not a hazard.

>Overall, I found these standards funny, not useful. My conclusion is that no  
>safety critical software can not be written in the UK since points 1 and 2  
>will mean that none of it will be up to standard.

I cannot understand how this conclusion follows. There is already software performing safety-critical functions that satisfies these standards. In my experience, the software that has killed people in the past has almost always used unnecessarily complex programming techniques. For example, the Therac deaths were related to race conditions in the software created by the use of multitasking (which was not necessary to implement the required functionality). The nondeterminism involved makes it impossible to thoroughly test or analyze the Therac software to eliminate such critical errors.

The most effective way to increase the reliability of software that we currently know about is simply to make it understandable and predictable. Although there may be many very good reasons for using sophisticated programming techniques, increased reliability and safety are usually not among them. When human life is involved, most real systems make tradeoffs in the direction of simplicity and predictability.

For the most part, the new UK standard just specifies current standard practice for safety-critical software used by those most experienced in building such software.

nancy

---

## Errors in weapon software

<JON.JACKY@GAFFER.RAD.WASHINGTON.EDU>

3 Jul 1989 17:19:30 EST

At the COMPASS '88 meeting last summer, John Cullyer described a quality study on modules selected from the NATO software inventory that was performed at the Royal Signals and Radar Establishment (RSRE), the central electronics research laboratory of the UK Ministry of Defence (MOD). Here is mention of that study from a recent paper, "High Integrity Computing", by W.J. Culler, pages 1-35 in "Formal Techniques in Real-Time and Fault-Tolerant Systems (Lecture Notes in Computer Science No. 331)", edited by M. Joseph, Springer-Verlag 1988:

``One of the techniques which has been developed to provide objective evidence of the correctness of software is called `static code analysis' ... (which uses) algebraic methods which are totally independent of dynamic testing...''

Application of static code analysis since 1985 has revealed some worrying results. Taking a broad average over the software checked by MOD or by contractors on behalf of MOD, up to 10 percent of the individual software modules have been shown to deviate from the original specification. Such discrepancies have been found even in software that has been subject to extensive testing on multi-million pound test rigs. Many of the anomalies detected have been minor and did not threaten the integrity of the system being monitored.

However, about 1 in 20 of the defective functions that static code analysis had shown to be faulty, i.e., about 1 in every 200 of all new modules, proved to have errors that would have resulted in direct and observable effects on the vehicle or plant concerned. For example, potential overflows in integer arithmetic appears to be a common problem, involving a change in sign of the result of a calculation and hence the possibility of an actuator being driven in a dangerous direction."

At COMPASS, Cullyer said about the same proportion of faulty modules was discovered in the British, American and German contributions. He also mentioned that the British MOD's interest in formal methods was motivated by several near-miss accidents involving computers that he said he was not permitted to discuss.

- Jon Jacky, University of Washington

---

### **✶ Where does safety lie?**

*jennifer s turney <turney@cetus.crd.ge.com>*

*Fri, 7 Jul 89 08:22:31 EDT*

In a TV news report last evening (7/6) on the computer shutdown at O'Hare Airport, the reporter commented that the skies were actually safer as a result, which he attributed to two causes: first, that there was less air traffic and second, that "pilots are relying on their knowledge and their skills rather than on a computer."

Jennifer Turney

---

## **✂ SP Cajon crash**

Mike Trout <miket@brspyr1.brs.com>

Fri, 7 Jul 89 11:22:25 EDT

The investigation continues into the Southern Pacific May 11 Cajon wreck. This was the incident where an SP potash unit train lost its brakes while descending Cajon Pass, a grade in excess of 2%. The train roared down the hill as the crew radioed they were out of control; it reached 90 mph before jumping the track and crashing into a neighborhood near San Bernadino. Three persons were killed, eight injured, and 11 homes destroyed.

New information indicates an inaccurate calculation of the train's tonnage. Press reports indicated the train contained 69 cars with a weight of 6150 tons, but an SP assistant chief dispatcher has since estimated the actual weight as 8950 tons. Had the crew known the train's additional weight, they might have set up the air brakes sooner. Faulty dynamic brakes were found in one of the four lead engines and one of the two pushers. As the train crested the hill, the lead engineer radioed the pusher engineer to ask if he was "giving all [the dynamic braking] he had;" the rear engineer answered "yes" even though he told investigators that he was aware the dynamic brakes were not working.

--From \_Call\_Board\_, Mohawk & Hudson Chapter Nat'l Rwy Hist. Soc.

Michael Trout, BRS Information Technologies, 1200 Rt. 7, Latham, N.Y. 12110

---

## **✂ Re: Stalking the wary food shopper**

<denbeste@BBN.COM>

Mon, 10 Jul 89 16:38:56 -0400

David Gursky's comments about grocery stores using computers to keep track of their customers so as to target mailings isn't anything new.

I can't be the only person who wasn't allowed out of a Radio Shack store until I gave my name and address...

And I always say "I'm on the mailing list already" and they always say "Well, the computer will notice it and won't put you on again."

Problem is, my name is just complicated enough so that there's always just a LITTLE bit of difference when it is keypunched, and the computer says "BING BING BING not the same; add it to the list."

Steven C. Den Beste (right. "Den Beste" complete with embedded space is my last name.)

Steven C. Denbeste, Steven Den Beste, Stephen Den Beste, Steven D. Beste, Steven Dan Beste, Steven Beste, Steve Den Beste, Steven Baste, and on and on and on. At one address I was on the damned list 5 times. And since the Radio Shack mailing list never dies (they always say "or current resident") some poor bastard is STILL getting those five catalogs every couple of weeks.

[I think I won't sign this.]

[At least he did not want it to be anonymous! PGN]

---

**✉ Re: Stalking the wary food shopper**

David Gursky <dmg@lid.mitre.org>

Mon, 10 Jul 89 19:45:50 EDT

The best comment of all may be that I received Steve "Pick a last name" Den Beste's message \*before\* my copy of RISKS with my message arrived!

And if it is any consolation to Steve, in all the times I have shopped at Radio Shack (albeit few times) I have yet to receive their catalogue in the mail.

---

**✉ Re: Stalking the wary food shopper**

<asente@wsl.dec.com>

Mon, 10 Jul 89 14:37:57 PDT

A less-intrusive variant of this is already in place at my local Safeway. After your purchase is rung up, a little printer on top of the cash register spits out some coupons for you. They always are for competing brands of things similar to what you just bought.

---

**✉ ORAIS'89 Conference Program**

Klaus Brunnstein <brunnstein%rz.informatik.uni-hamburg.dbp.de@RELAY.CS.NET>

30 Jun 89 14:40 GMT+0100

International IFIP-GI (IFORS-EFMI-AIME-GMDS) Conference: Program  
Opportunities and Risks of Artificial Intelligence Systems (ORAIS'89)

July 17-20, 1989; University of Hamburg, FR Germany

Monday, July 17, 1989: AI History, Impact, Paradigms  
J.Weizenbaum(Boston): Historical Perspectives of AI+changing Paradigms  
R.Lauffer(Jouy en Josas): The Social Acceptability of AI  
W.Bibel(Darmstadt): AI + Change of Reality: Opportunities+Dangers  
Afternoon: Working Groups: Position Papers

Tuesday, July 18, 1989: Expert System: Opportunities and Risks:  
S.Savory(Paderborn):Expert System Vision: Reality vs. the Hype  
J.Berleur(Namur): CoSpeakers Comments  
W.Coy(Bremen): Machine Intelligence + Industrial Work  
B.Radig(Munich): CoSpeakers Comments  
Afternoon: Working Groups: Position Papers

Wednesday, July 19, 1989: Applications of AI  
M.Stefanelli(Pavia):AI in Medicine

H.Fiedler(Bonn): AI in Law  
Sture Haegglund(Linkoeping):On the Impact of Intelligent Systems  
and Knowledge Management Support in the Office Environment  
H.Sackman(LA):Salient Internat.Socio-Economic Opportunities+Risks in AI  
Afternoon Socio-Cultural Event (Ship tour to Operation Sail'89)

Thursday, July 20, 1989: Conference Results and Outlook:  
Working Group Result: Report of WG Chairpersons  
K.Brunnstein(Hamburg): Human Intelligence and AI: an Outlook

Working Group 1: Building Knowledge Bases & Expert Systems

A.Kobsa(Saarbruecken):User Modeling in Dialog Systems:Potentials+Hazards  
T.Bub (Darmstadt): Artificial Intelligence is an Information Technology  
B.Becker(St.Augustin):Elicitation+Modelling of Expertise:fundamental limits"

Working Group 2: Applications in Medicine:

J.Mira Mira(Santiago de Compostela):Time Aspects of Therapy Advisors  
L.Gierl(Munich): Experiences in Use of Expert Systems in Medicine  
H.Woltring(Eindhoven): Software+AI:How free are Research+Development?  
R.O'Moore(Dublin): Evaluation of Expert Systems in Medicine  
P.Nykanen(Tampere/Finland): The SYDPOL Project  
J.John(Munich): Methodological Aspects of TA on Expert Systems in Medicine  
R.Engelbrecht(Munich):Opportunities+Risks of ExpS: Results from 3 Studies

Working Group 3: Applications in Enterprise

A.Leifeld(Duesseldorf):Using an ExpS to hedge Foreign Exchange Exposure  
M.Daniel(Karlsruhe): Impacts of Commercial Applications  
H.Damskis(Paderborn):The only Risk is not to take the Opportunity

Working Group 4: Office Applications

H.Brinkmann,A.Hohmann(Kassel):Decision Support Systems in Complex  
Organisations (Job Placement at Employment Offices in FRG)  
P.Dambon,F.Glasen,R.Kuhlen,M.Thost(Konstanz):Risks+Opportunities of  
ExpS in Offices of Administrative Institutions(Creditworthiness Tests)  
G.Unseld(Frankfurt):Elementary Logic of Risks+Chances in the AI Business

Working Group 5: Industrial and Engineering Applications

P.Broedner(Karlsruhe):In Search of the Computer Aided Craftsman  
W.Beuschel,B.Groeger(Berlin/FRG):Chances+Risks of Using ExpSystems  
in the Engineering Design Process  
G.Stein(Leonberg/FRG):Why are Automatic Image Analysis Systems so limited?  
J.Heikkilae,P.Heino(Tampere):Risks of Industrial Systems with Knowledge  
Based Software  
S.Klaczko,M.Goeller(Hamburg):Automatic Reasoning for Decision Support  
Systems: the CIM Case

Working Group 6: Public and Legal Aspects

B.Brauner(Koeln): Some legal Aspects of ExpSystems according to German Law  
W.Kilian(Hannover):Liability for deficient Medical Expert Systems

Working Group 7: Education & Training:

M.Angelides,G.Doukidis(London):The Effectiveness of AI in Tutoring Systems  
D.Millin(RamatHasharon):Are Educational and Training Systems threatened  
by new Technologies such as AI and ExpSystems?

Working Group 8: Risks and Security of AI-Systems

I.Georgescu(Bucharest/Romania):Risks Sources in AI Applications

H.Goorhuis(Zuerich):NESSY: A System that combines Symbolic Reasoning  
and Neural Computing to avoid some Risks of ExpSystems

S.Fischer-Huebner,K.Brunnstein(Hamburg):Opportunities+Risks of Intrusion  
Detection Expert Systems

A.Kieback,W.Vogel(Friedrichshafen):On Security of AI Systems(Experiences)

Working Group 9: Risks and Accountability:

K.Roediger(Berlin):The GI Document 'Computers and Responsibility'

H.Sackman(LA): Towards an IFIP Code of Ethics based on Participative  
International Consensus

Working Group 10: Methodological Aspects:

G.Knospe(Wismar/GDR):Cognitive Adequacy of Knowledge Representation

K.Fuchs-Kittowski(Berlin/GDR):Philosophical+Methodological Positions  
regarding the Relationship between Artificial+Natural Intelligence

Working Group 11: Software Technology Impacts

H.Mueller-Merbach(Kaiserslautern): Intelligent Man-Machine Tandems

C.Pyka(Hamburg): Future Information Systems for Everybody

R.Meyer,W.Rose(Hamburg): CASE for the Nineties

G.Dimitriou(Thessaloniki): AI in Software Engineering

Conference Location: Hamburg University, Rechtshaus

Schlueterstrasse 28, D 2000 Hamburg 13, FR Germany

More information available from:

Conference Secretariat: Dr. Klaus Brunnstein (Program Committee)

Simone Fischer-Huebner (Organisation Committee)

University of Hamburg (ORAIS '89),Schlueterstr.70, D 2000 Hamburg, FRG



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

**Volume 9: Issue 4**

**Thursday 13 July 1989**

## Contents

- [Air Traffic Computer Fails 104 Times in a Day](#)  
[Rodney Hoffman](#)
- [A320/MD-11 F-B-W differ on pilot authority](#)  
[Mark Seecof](#)  
[Rodney Hoffman](#)
- [UK MoD S/W Std -- "Crystal Clock" Architecture](#)  
[Bob Munck](#)
- [A Biological Virus Risk](#)  
[Frank Houston](#)
- [Software engineering models -- an apology](#)  
[Rich D'Ippolito](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ***✉* Air Traffic Computer Fails 104 Times in a Day**

*Rodney Hoffman* <[Hoffman.ElSegundo@Xerox.com](mailto:Hoffman.ElSegundo@Xerox.com)>

*12 Jul 89 07:59:01 PDT (Wednesday)*

Summary of an article by Jeffrey A. Perlman in the 'Los Angeles Times' 12 July 1989 is headlined AIR TRAFFIC COMPUTER FAILS 104 TIMES IN A DAY:

Unspecified hardware problems caused 104 brief failures in a new multimillion-dollar computer system throughout the day Sunday at the Coast Terminal Radar Approach Control, known as Coast TRACON, in El Toro. The failures, up to five minutes in length, wiped altitude, speed, aircraft identification, and radio frequency data off of controllers' screens, leaving only aircraft blips or targets.

The new system has no backups, unlike the aging system it replaced 2.5 months ago. Furthermore, a decoder which could have provided some of the lost information from aircraft transponders, is inoperative because parts are on back order. During the failures, controllers had no way of knowing an aircraft's altitude or identity except through voice communications.

Controllers said the failures endangered air safety, although the FAA minimized the hazards. Although there were no "near misses," many aircraft departing from LA International airport did encounter short delays because controllers were swamped.

An emergency technical crew was flown in from New Jersey and worked all night Monday to correct the problem. A controller spokesman said there were still at least three more failures as of Tuesday afternoon, although the FAA's assistant regional manager said he was unaware of any further computer failures after Monday night's repairs.

The National Air Traffic Controllers Association has previously filed complaints with the FAA about the El Toro system and about TRACON facilities elsewhere that have received the same system.

[MORE SUBSEQUENTLY FROM RODNEY:]

The previously unspecified hardware problems are now spelled out: According to Jim Panter, manager of the facility, "no new computer system was involved. It was strictly old equipment that needed to be replaced." The series of computer outages was traced to four brittle, broken wires inside aging memory storage units. Four of the Univac computer's 11 memory modules, in use for at least 12 years, went out on Sunday because of the wires. A heat build-up aggravated the situation, with the computer system shutting itself down and restarting, catching up with new data, as it tried on its own to locate the memory storage problem.

A special crew from the FAA's technical center in Atlantic City, NJ, worked on successive nights this week to solve the problem, but because of a parts shortage some outages still occurred Monday and Tuesday, Panter said. There were no outages Wednesday, he said.

The computer system involved has been in use at least since 1972, although it has been upgraded several times with new software. The software was not involved in Sunday's failures, although it has been involved in problems at other TRACON facilities. "Just like any program, the new software has had its glitches," said FAA spokesman John Leyden in Washington.

[This item was also noted -- briefly -- by Dave Curry. PGN]

---

### **A320/MD-11 F-B-W differ on pilot authority**

<icc.marks@SEAS.UCLA.EDU>

Wed, 12 Jul 89 11:23:44 PDT

These excerpts from "Flying the Electric Skies," M. Mitchell Waldrop, Science (30 June 1989, p.1532ff, v.244). Elisions... and [bracketed paraphrasing] are mine as part of condensation. Comments follow.

[...] McDonnell Douglas... thinks [pure fly-by-wire isn't quite mature, so it's]... taking a different tack with its new MD-11, a three-engine widebody scheduled to start service in late 1990. The MD-11 is even more highly

automated than the A320 in many ways. ... But the MD-11's computerized controls most emphatically will have mechanical backups. "The pilots have to have control in all situations, not just the normal ones," says Douglas' Miller. "A lot of what ended up in the Airbus got done because it was neat," claims Joel Ornelas, manager of the MD-11 design effort. "Engineers love it. But the pilots...?"

[...] Airbus [doesn't agree. They think their stuff is great and saves weight and can't fail; but]... the A320 does have a partial backup system: a set of cables running back to the tail and rudder. In an absolute power failure those cables are supposed to let the crew keep the airplane under control until they establish emergency power--or if need be, longer. "In test flights we've demonstrated {operation with the backups} from cruise... to landing... which is more than they were designed to do."

[... However, the pilot of an A320] is... going to have to live with the A320's preprogrammed restrictions on what it will do. This guardian angel behavior, known more formally as the Flight Envelope Protection System, is widely considered by aviation professionals to be... far more revolutionary... than fly-by-wire per se. In effect, the A320's designers have decreed that their judgement about the aircraft's limits will always take precedence over the pilot's judgement. And that is not a constraint that any pilot can take lightly.

"\*Nothing\* must have the authority to forbid the pilot to take the actions he needs to," Says McDonnell Douglas' Miller. The problem with giving away that authority to a computer, he says, is that "a computer is totally fearless--it doesn't know that it's about to hit something."

Imagine, for example, that an A320 pilot makes a sharp turn to avoid an imminent collision, or else dives and then has to pull out to avoid the ground. No matter how desperately he or she hauls back on that sidestick, the envelope protection system will not let the airplane respond beyond a certain rate: namely, the rate that limits stress on the airframe to... 2.5G.

...this seems like plenty. [It would] require quite a violent maneuver [to pull 2.5G]. ...But consider... China Airlines Flight 006 on 19 February 1985. While cruising at 41,000 feet some 300 miles NW of San Francisco... the 747 suffered [power loss and cockpit confusion leading to a] near vertical dive. Over the next three minutes it plunged nearly 6 miles, until the captain was able to maneuver it back into level flight at only 9500 feet. He measurably warped the wings. He caused several million dollars worth of other structural damage. But he saved the airplane and passengers. And to do it he had to pull an estimated 5.5G, or more than twice the A320 limits.

Airbus, not surprisingly, responds that an A320 never would have [entered the dive] in the first place. ...Be that as it may, notes [747 pilot] Waldrip, many pilots do like to feel that they can bend or break the aircraft [if they must]. [McDonnell Douglas agrees.] "Our strategy... is that the pilot must have overriding authority," says Miller, "and he must be able to exercise that control by the normal method"--the same eye-hand-brain control loop that a pilot develops through... experience.

For example, imagine a pilot caught by wind shear, a sudden and very

dangerous burst of cold air falling out of a rain cloud. The best thing to do in such a situation is to pull the nose up and put the power to the wall. Never mind if the engines have to be rebuilt later; you're just trying to keep from hitting the ground. However, this is hardly the time to be thinking about things like special override switches, says Miller. "You want your normal... actions to always have the expected effects." So on an MD-11, the pilot would push the throttle all the way forward until it stopped to get the full rated power of the engine, with the built in limits providing the same kind of security as the A320's envelope protection system. But then by doing the instinctive thing-- pushing very, very hard-- he could break through to a regime the A320 absolutely forbids: extreme thrust, well beyond the rated power. And so it goes throughout the MD-11, says Miller. The limits are there for safety, "but to override you just have to pull hard or push hard." [...] The Mac-Dac engineers seem to have worked hard on the "human-factors" stuff. I'm struck by the thought that 'push hard to override' is rather like "pounding on things," which has sort-of appeared in office computer interfaces; for example... giving a likely-to-be-an-error command to the vi text editor will provoke a message the first time you try it, but if you repeat the command immediately vi will shrug and do what you want.

It seems to me that risks from faulty computer-human interaction probably can be reduced by this sort of thing. When time is critical, it's handy if "more force" gets you what you want without fumbling around for some obscure override control.

The issue of "who's in charge here, anyway?" is more interesting. The A320 approach assumes that pilot error is more likely than proper-thought-unusual control motions. Since pilots are still more versatile than the computers in their planes, they should probably have the last word. Also, pilots can learn new tricks faster than computers can receive certified software upgrades. Post-aircrash review (and recently, simulator recreation/experimentation) often produces "how-to" bulletins for pilots to deal with unusual situations. It might be a long time before that stuff could be translated into revised FCS software.

Mark Seecof, Locus Computing Corp. Los Angeles (213-337-5218)  
My opinions only, of course...

---

### Fly-by-wire overview

*Rodney Hoffman <Hoffman.ElSegundo@Xerox.com>  
12 Jul 89 14:52:10 PDT (Wednesday)*

[More excerpts from the same 'Science' article as in the foregoing... PGN]

The stories briefly survey the philosophy, state of the art, and controversy of fly-by-wire aircraft and (overly-?) protective new extensions. Designers on both sides of the argument, as well as pilots, are given their say. [...]

Airbus engineering test pilot Udo Guenzel: "Suppose you suddenly find yourself staring at a Cessna that has wandered into your airspace. So you swerve. Now, in a standard airliner, you would probably hold back from

maneuvering as hard as you could for fear of tumbling out of control, or worse.... But in the A320, you could just slam the controller all the way to the side and instantly get out of there as fast as the plane will take you."

The A320 has five separate computers, "redundant software obtained from two different vendors to minimize the possibility that the same bug will appear simultaneously," heavy shielding on its data cables to keep out electromagnetic interference, "and, yes, the A320 does have a partial [mechanical] backup system."

The sidebar reviews more of the history of fly-by-wire and flight automation philosophy:

"We started out with cockpit automation backwards," says Northwest Airlines 747 pilot Kenneth Waldrip. In the 1970s and early 1980s, he says, "the idea was that the computers would fly the plane and the pilot would monitor them in case anything went wrong...." There was only one problem with that scenario, Waldrip says: humans are absolutely terrible at passive monitoring.... People get bored. Their attention flags. They start missing things. Worse, a passive pilot would often have to tackle an emergency cold....

By the mid-1980s, aircraft designers, pilot trainers, and the aviation community generally had gone through a 180-degree turn in their concept of what automation should do. The new philosophy, which often goes under the name of "human-centered" automation, was illustrated in 1980 in a seminal paper by human factors researchers Earl Wiener (Univ. of Miami) and Renwick Curry (NASA Ames Research Center). They used the image of an "Electric Cocoon" [similar to the Flight Envelope Protection System of today's A320].

Instead of having people watch the machines, human-centered automation means having the machines watch the people.... and it means putting automation back on the right track: as an assistant to the pilots.

---

## ✂ UK MoD S/W Std -- "Crystal Clock" Architecture

Bob Munck <munck@mbunix.mitre.org>

Thu, 13 Jul 89 14:31:52 EDT

I can't let go unchallenged Norm Finn's and Nancy Leveson's statements ([RISKS-9.2](#), .3) on what are variously called "polling," "time-slot," or "crystal clock" system architectures:

"Polling is absolutely the safest and most-used method for programming embedded systems for safety-critical applications."

"The trivial scheduling algorithm makes the interaction between the routines vastly easier to write and verify than is the case in a system that can switch tasks at random times."

"Software with these characteristics is safer because it is

deterministic rather than non-deterministic -- the number of states may often be reduced to a small enough number to perform extensive (and sometimes exhaustive) testing and analysis."

I don't want to comment on the \_theoretical\_ truth of these statements; that argument may never be resolved. However, in my personal experience with major DoD systems over many years, this approach to system architecture has led to many more absolute abominations than any other.

AAAAAAAAAAAAAAAAAAAA

The major problem, I believe, is that it does not work well with normal design and coding team organization and management. The approach AS PRACTICED seems to grind together the pieces of any original functional organization, breaks them into small pieces, and then "shotguns" them all over the time-slot hierarchy. Traceability from requirements to code, never our strong suit, is lost. "Invisible dependencies" become the order of the day: code in major cycle XXYa34/minor cycle Ybbb\_CAL assumes that variable IXXm3\_AP was set correctly by a side-effect of code in XXZdd3/PQ88\_SET/ECP9347q; when XXZdd3 is reorganized because it wasn't fitting in its time-slot, the assumption became incorrect. This is first noticed when the \$100 million satellite attempts to orbit at -800 miles altitude. Because our teams are large, scattered, ill-managed, and leavened with the mediocre, the possible advantages quoted above are overwhelmed.

I feel about these dueling approaches as I do about HOLs: a good programmer/team/company can write a good system in any language, and a bad one can write a bad system in any language. The time-slot systems I've seen might have been even worse had they been designed to be multi-tasking; the choice of architecture was not the root cause of failure. It may be a symptom.

-- Bob Munck, MITRE Corporation, McLean

---

## **A Biological Virus Risk**

*Frank Houston <houston@itd.nrl.navy.mil>*

*Wed, 12 Jul 89 12:54:43 -0400*

Over the past six years, FDA has documented an increase in medical device problem reports of and voluntary recalls for system design errors and computer programming errors. Some of the reported errors have compromised patient safety. Included are blood bank computer systems used in controlling the release of whole blood and blood products for treating patients. Some of the errors could have allowed institutions to release infected blood products.

Such inappropriate release is particularly hazardous to the public health because blood products infected with HIV (AIDS virus) and hepatitis might become available for transfusion. Fortunately, so far, no cases of HIV infection have been traced directly to computer errors, but agency experts and field investigators believe this result is only because the institutions have not depended

heavily on software controls to authorize release of blood products.

One particularly troubling aspect of the problem, uncovered during an inspection, was a lack of security on serologic data entries. The system allowed more than one operator to edit the same record simultaneously, with the result that the last one to close the record had the final word on the contents of the record. That is to say, one operator could enter a test result of positive for hepatitis and exit while at the same time a second operator entered some other result (the default hepatitis result being negative); so when the second operator exited, the default negative for hepatitis became the permanent entry. This seems to violate well known principles of data integrity, but it happened.

The software in question is no longer used, but the problem remains: how does one assure that dangerous bugs have been eliminated from commercial software when one has neither real-time information about nor control over the way it is developed?

Frank Houston, FDA/CDRH

---

### **✂ Software engineering models -- an apology**

<rsd@SEI.CMU.EDU>

Wed, 12 Jul 89 17:25:50 EDT

[The lateness of this response and to my e-mail is due to a city watermain break that flooded the basement of the building with the cooling equipment in it, shutting down our building for 6 days -- as noted in [RISKS-9.1](#).]

First, let me apologize to Stan Shebs and the readers of RISKS for the tone and content of my recent article. It was not intended to be a shoot-the-messenger reply, and I'm sorry that it appears to be. I most likely read the original article as an series of general unsupported charges against a specific former employer who had no way to respond, and took my cue from the clearly provocative title.

Let me make the attempt to extract some lessons from the original article and all of the subsequent discussion:

Mr. Loux asks if the intent was to discourage whistle-blowers. Of course not; I didn't take the article as whistle-blowing to begin with. The intent was to elicit more specific information on exactly what the charges were and who they were against. Many of the statements were made with little or no support other than admitted hearsay, and I'm sorry I didn't respond to the message instead the statements. I will disregard those statements in the remaining discussion.

It was not clear to me that there was a connection between the "model" software engineering methodology and the file transfer problem -- I should not have missed that. Mr. Shebs's clarification of this point and expansion to the comparison of meeting the letter of DoD acquisition requirements with software quality should be seen as evidence for the immaturity of the SE

discipline everywhere -- not just for the defense industry.

It is the real lack of true engineering methods that leads to the acceptance of "models" where the emphasis and attention is placed on the checking off of boxes on a delivery schedule. After all, the incentive structure is set up to reward schedule adherence, so it is easy to predict that the efforts will be devoted to getting the all of boxes checked at the right times. How can you fault the management for doing what they are paid to do? Even a well-educated management (in terms of technical realism) will have a hard time making the right response under such reward conditions. Many non-defense contractors have found that offering the programmers extra rewards for meeting schedules does not get better software, nor does it get it on time, when the impossible is requested.

Mr. Shebs also states that the greatest risk might have been from things that weren't anticipated during testing. I suggest that waiting until testing is too late. The time to do the risk analysis is in the initial stages of design, so that the testing procedures are only used to verify that the implementation is faithful to the design. It is because there is not the clear separation of design from implementation in the software industry that testing is misunderstood and misused.

The issue of problem reports and their unclear relationship to software quality is also a result of the failure of traditional methodologies to separate design from implementation, and from their nearly exclusive focus on process. The best process in the world can't be expected to do more than produce economical, consistent copies of poor designs! The problem will be with us until we shift from process orientation to product orientation.

I would like to take issue with Mr. Loux's characterization of the problem as being inherent in engineering. True engineers do not respond to absurd or impossible situations. Engineering, as an applied science, has been the basis for reasonable expectations, as engineers are adverse to undertaking projects of any kind without having a base of working models of prior solutions (captured scientific knowledge) to adapt. Without such models, there is nothing on which to build a set of application techniques to apply the knowledge, let alone a way to generate a rational set of tests and expectations for the final product.

Which company, defense or otherwise, will be the first to refuse to bid on a project requiring technology that it has never delivered, and which software engineers will be the first to refuse to agree to deliver something for which no models have been proven?

Rich



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

**Volume 9: Issue 5**

**Saturday 15 July 1989**

## Contents

- [UK Defence Software Standard](#)
  - [Dave Parnas](#)
  - [Nancy Leveson](#)
  - [Dave Parnas](#)
- [DARPA contract: use AI to select targets during nuclear war](#)
  - [Jon Jacky](#)
- ["Flying the Electric Skies"](#)
  - [Steve Philipson](#)
- [Automobile Electronic Performance management](#)
  - [Pete Lucas](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **✉ UK Defence Software Standard (Nancy Leveson, [RISKS-9.3](#))**

*Dave Parnas <parnas@qcis.queensu.ca>*

*Thu, 13 Jul 89 22:07:37 EDT*

Nancy Leveson suggests that eliminating dynamic memory allocation, recursion, interrupts and multi-processing is done in safety critical systems to make them deterministic. I disagree. Software that uses those techniques can be just as deterministic as software that does not. Further, software without any of those features can be non-deterministic in its behaviour. For example, the non-determinism associated with interrupt handling comes from the unknown timing of the external events and is not affected by the replacement of interrupts with polling.

The MOD restrictions do not rule out non-determinism. Further, they do not rule out bad programming. If I am forbidden to use compilers or operating systems with dynamic memory allocation and consequently write complex programs that use "static" variables for many different purposes I am likely to introduce more mistakes than would have been present in the mature dynamic allocation system that I was not allowed to use. If, because I am forbidden to use recursion, I write a complex program that does the stacking and backtracking hidden by recursion, I am likely to introduce more errors than

were present in the compiler's well-tested implementation of recursion. Similarly, if I introduce busy waiting and polling in my programs because I cannot use interrupts, I may again make things worse rather than better.

Nancy is right in saying that "it is simply untrue that these limitations rule out real systems." Many perfectly horrible real-systems have been written without any of those features.

Nor, would I agree that non-determinism is bad. Non-determinism has been demonstrated by Dijkstra (and much earlier by Robert Floyd) to allow programs that are much more easily verified than some deterministic ones.

These regulations remind me of the old story about a man found looking carefully under a street lamp. When asked, he said he was looking for a coin he had dropped on the other side of the street. When asked why he was looking on this side, rather than where he dropped the coin, he replied that it was too dark over there.

Regulations of this sort are imposed not because they are the right restrictions but because they are easily enforced by people who do not want to read programs carefully. It is much easier to verify that recursion and interrupts have not been used than to verify that the program is well-structured, well-documented, systematically inspected (verified), and adequately tested. Just as it is easier to look for a ring under a street light, it is easier to check for the absence of features than the presence of quality.

All my knowledge of the Therac software comes from discussions with Nancy. However, from her description the problem with that software was not the use of multi-tasking but the failure to use well-known (and well-understood) ways of making multi-tasking verifiable.

As Nancy says, "The most effective way to increase the reliability of software that we currently know about is simply to make it understandable and predictable." "Sophisticated programming techniques", properly used, can do just that. Unfortunately, we cannot make regulations that define "properly used" so some of us are throwing the baby out with the bath water.

David L. Parnas

---

## UK Defence Software Standard

*Nancy Leveson <nancy@ICS.UCI.EDU>*

*Fri, 14 Jul 89 16:08:56 -0700*

I have great regard for David Parnas and his opinions, but we do have a difference of opinion with respect to this issue.

Perhaps I am using the term "non-deterministic" incorrectly. When interrupts are used, it is not possible to pre-determine in exactly what sequence the statements of the software will be executed because the interrupt-handling code can be executed at any time. When using polling, the programmer has

more control over when the input-handling code is executed. It is possible to use priorities to ensure that the code to abort a missile launch is not interrupted, for example, but this just complicates things further and introduces the possibility of different types of errors. At the least, limiting the possible execution sequences allows for more extensive testing given a fixed amount of testing resources. It also allows for more reliable timing analysis as pointed out by someone in a previous posting to Risks. Am I misunderstanding something here?

With respect to Therac, it is true that the errors were involved in multi-tasking and its poor implementation. But the use of the "well-known and well-understood ways of implementing multi-tasking" do not guarantee errors will not be introduced. You are assuming that they would implement those features correctly. Although I have great confidence that David Parnas or Edsger Dijkstra could use ANY techniques with great skill, I have less confidence that this is true for all the programmers writing military software.

David is obviously right that using recursive constructs is safer than implementing recursion oneself with stacks and backtracking. But it would be safest (in terms of all types of potential faults including run-time stack overflows) to try to find a simple, non-recursive algorithm to accomplish the same thing. If one does not exist, then the argument for this should be included in the certification procedure. It is easier to grant dispensations to standards when someone provides an argument that it is safer to do so than it is to try to check all software to ensure that superfluous complexity has not been introduced. The person arguing to certify their software must then provide good arguments for introducing complexity rather than the certifier having to determine whether simpler designs exist. Remember, we are talking about a potential nuclear armageddon here and with certifiers who may be no more knowledgeable than the programmers.

David is also right that it is better to check for the presence of quality than the absence of features. I would hope that standards would require that quality be built-in and assessed and not just include these simple rules. Unfortunately, I have no way of looking at a program, even a well-designed one, and guaranteeing that there are no errors in it. I do have more confidence that people will make fewer mistakes when their programs are simpler and when they use techniques that rule out various common types of errors. For example, if the design they choose does not involve the potential for deadlock, then I need not worry about it occurring. If the man had carried his coin safely ensconced in his wallet, he would not have had to look for it on either side of the street. Sure, as David says, "perfectly horrible real-systems have been written without any of these features." That is exactly why such standards should contain more than just simplistic rules. But that does not mean that rules are not also useful in the context of an imperfect world.

I guess our disagreement comes down to the following: Assuming David's belief that these techniques, properly used, can increase reliability, is it more likely that errors will be introduced (1) because they are improperly used or (2) because they are not used at all? Until we have experimental data on this, it remains a matter of personal opinion.

It would be nice if the people who introduce these programming techniques and argue that they increase reliability would do comparative studies to confirm their claims. This type of experimentation is very difficult (as we have found out by trying to do it), but long overdue in our field.

Nancy G. Leveson

---

### **✂ UK Defence Software Standard**

*Dave Parnas <parnas@qucis.queensu.ca>*

*Fri, 14 Jul 89 22:05:28 EDT*

I have great respect for Nancy Leveson's work and for the great effort she has put into increase everyone's awareness of safety issues, but we continue to have a difference of opinion here.

1) In fact, hardware interrupts are simply hardware implemented polling and the use of interrupts gives the programmer control (because of more rapid response) than can usually be achieved by software polling. Nancy's impression that the programmer loses control comes from the fact that we often use interrupt response code written by others (operating system code) and consequently feel that we have less control. If we allowed someone else to write the polling code, and the code to respond when an event was detected, we would be in exactly the same situation, except that there would be a slower reaction time. Both software polling and interrupt handling can be done badly and both can be done well.

Edsger Dijkstra's 1968 papers showed how an interrupt handling system could be set up in a way that the programmers could restrict the order of events as much as they wish. Moreover, the beauty of his approach was that most of the software was unaffected by the choice between interrupts and software polling. The P and V interface hid the difference between events detected by hardware and those detected by software. Twenty years later I meet people who are called "software engineers" but have no knowledge of that work or understanding of similar techniques. Today's hardware and software technology would allow us to do even better than was possible in 1968.

2) Nancy is wrong when she states that I am assuming that programmers would implement those ideas correctly. I have too much experience to make such an assumption. She could equally well be accused of assuming that programmers will avoid those ideas "correctly". There is no idea so good that it cannot be used badly.

3) No one is more in favour of the use of "simple algorithms than I. My vitae carries a quote from A. Einstein, "Everything should be as simple as possible, but not simpler". Further, I don't even believe that there are such things as recursive programs. They are all iterative programs in disguise. I do however find that recursive descriptions of programs are often simpler, and easier to verify, than iterative descriptions of the same algorithm. We must never forget the "but not simpler" phrase in Einstein's remark.

4) If Nancy thinks that the danger of deadlock is caused by multi-programming I must also disagree. Every program built using pseudo-parallel processes has an equivalent "sequential program" that can exhibit exactly the same abortive behaviour as its deadlocking counterpart. If Nancy, thinking that deadlock is impossible because there is no multi-programming, does not look for those errors, she will just be surprised and dismayed when the program enters an unending loop or a permanent idle state at unexpected times.

I believe that organisations such as MoD would be better advised to introduce regulations requiring the use of certain good programming techniques, requiring the use of highly qualified people, requiring systematic, formal, and detailed documentation, requiring thorough inspection, requiring thorough testing, etc. than to introduce regulations forbidding out the use of perfectly reasonable techniques.

Like Nancy, I wish we had experimental data to confirm or disprove my belief in the potential of these techniques but I don't expect to get such data. Other differences, such as the qualifications and interest of the personnell will swamp the effect of the techniques that we are debating. Safety depends on the use of highly qualified, disciplined personnel for the design, documentation and inspection of softwre. By forbidding modern programming techniques, we could drive those people away and achieve just the opposite.

David L. Parnas.

---

### **✂ DARPA contract: use AI to select targets during nuclear war**

<JON.JACKY@GAFFER.RAD.WASHINGTON.EDU>

14 Jul 1989 17:39:10 EST

Here is a story from FEDERAL COMPUTER WEEK, July 10, 1989, pages 10,11:

DOD TARGET SYSTEMS FACE IMPROVEMENT by Gary H. Anthes

The Defense Department plans to improve substantially its planning system for the targeting of strategic nuclear weapons. As a first step, it is about to award a contract for a prototype system that would identify targets, allocate weapons and specify the timing and modes of weapons delivery.

DOD hopes to reduce the planning-cycle time from 18 months to three days, reduce personnel requirements by a factor of 10 and increase survivability by a factor of eight (see chart, below).

The overhaul of the process by which the plans are developed and changed during conflict reflects a shift away from large-scale use of nuclear weapons against fixed targets to more limited conflicts involving mobile targets. It also reflects recent presidential requests for more flexibility in the use of nuclear weapons.

The project, called Survivable Adaptive Planning Experiment (SAPE), is being funded jointly by the Defense Advanced Research Projects Agency and the Air Force. Prime bidders on the job are Harris Corp., McDonnell Douglas

Corp. and IBM Corp.

The United States' plan for nuclear warfare, called the Single Integrated Operational Plan (SIOP), is produced annually under the direction of the Joint Strategic Target Planning Staff (JSTPS), an element of the Joint Chiefs of Staff. The plans are developed at the headquarters of the Strategic Air Command in Omaha, Neb., using intelligence data, force-status information and guidance from the president, the secretary of Defense and other authorities.

``The president decides in broad terms the types of options and results he wants, and the JSTPS takes the guidance and produces the SIOP," said Army Lt. Col. Peter W. Sowa, SAPE project manager at DARPA.

SAPE is not intended to replace the initial planning process. Rather, it is geared to enabling rapid adaptation of the plan before and during a nuclear conflict while ensuring the survivability of the planning system. Sowa said: ``During a conflict, the situation will be different [from the one anticipated] especially if tactical nuclear weapons are used. Something is sure to be different, so you want to be able to replan quickly."

It now takes 18 months to create a new plan. Although it could be done faster, Sowa said, a completely new plan could not be developed in three days, which is the SAPE goal. Another SAPE goal is reducing the time required to change targets and to configure the planning network.

Retargeting time is of growing importance as the Soviet ballistic missile force becomes more mobile. ``Planning to hold fixed targets at risk is straightforward in concept but exquisitely complex in detail," the SAPE statement of work says. ``[But] when targets are capable of relocation over short time periods, accomodating those changes into strategic attack plans becomes enormously difficult."

SAPE specifications require the ability to change 600 targets per day during a nuclear conflict and to reduce the time required to change a target from eight hours to three minutes. The system also must be able to generate plan options involving 2,000 weapons and up to 4,000 targets in 30 minutes.

These objectives can only be overcome by powerful hardware, smart software and a high-speed communications network --- the cornerstones of SAPE. According to Sowa, the system will consist of several mobile processing clusters, each possibly consisting of a large mainframe or supercomputer, data base machines, parallel processors, and workstations. Each local cluster will be able to execute the whole plan, and each will connect to a survivable communications internetwork through a gateway.

The core software, most likely written in Ada and Lisp, will consist of mathematical algorithms and artificial-intelligence techniques, Sowa said. ``It will be a software development effort and an expert-knowledge-building effort. A lot of interviewing experts will be needed."

But the smart software will be of little use if the system is damaged during hostilities. By using redundant, distributed and mobile parts, DARPA aims to increase the system's tolerance to loss from 10 percent to 83 percent

and its communications connectivity during a conflict from 10 percent to 50 percent.

According to Sowa, the benefits of the more flexible SIOPs include the following:

- o Enhanced deterrence through the ability to hit mobile targets.
- o More efficient use of weapons. "If you don't shoot at empty holes, you don't need as many weapons," Sowa said.
- o Smarter wargaming. The system could be used to conduct what-if analyses - predicting the effects of different options --- as part of planning or negotiating processes.

Sowa said SAPE, which will require \$20 million to \$30 million over five years, is a demonstration project and is not intended to field a system. Some or all may be deployed, or the existing system might be enhanced in some other way, he said.

A contract will be awarded in about a month, and it will call for the design and development of an engineering development model. The model must be able to rapidly retarget and generate new options in an environment before a nuclear conflict. In subsequent phases, the model will be expanded to include those functions needed during a nuclear conflict and to create a new nuclear strike plan at the end of hostilities.

(This table accompanied the article:)

**SURVIVABLE ADAPTIVE PLANNING EXPERIMENT PERFORMANCE GOALS**

FACTOR	CURRENT	GOAL
Number of primary nodes	1	7
Time to replan full SIOP	18 months	3 days
Personnel resources	500 persons	50 persons
Retarget actions	10 per day	1000 per day
Time to retarget	8 hours	5 minutes
System tolerance to loss	10 percent	83 percent

**Communications connectivity**

Pre-SIOP	99 percent	99 percent
Trans-SIOP	10 percent	50 percent
Post-SIOP	30 percent	90 percent

Reconfiguration time      Hours      Seconds

(end of excerpts from FEDERAL COMPUTER WEEK)

- Jonathan Jacky, University of Washington

Steve Philipson <steve@eos.arc.nasa.gov>

Thu, 13 Jul 89 18:29:02 PDT

> [...] Airbus [doesn't agree. They think their stuff is great and saves  
>weight and can't fail; but]... the A320 does have a partial backup system:

"Can't fail"? This is pretty amusing. It's my understanding (possibly incorrect) that Airbus made this same argument about the A-320 control system before the manual backup systems were in place. The US FAA indicated that the A-320 would not be certified without those backups, no matter how reliable Airbus claimed the fly-by-wire system to be. Airbus gave in. During flight tests, the "can't fail" system suffered a total failure, and the A-320 prototype was flown using "peanut" self-powered flight instruments and the back-up manual controls (this event was reported in Aviation Week).

Airbus reports that the failure was a freak, they've fixed the problem, and that it won't ever happen again. Now it really can't fail. Right. Do we know that their analysis can't fail... again?

>No matter how desperately he or she hauls back on that sidestick, the  
>envelope protection system will not let the airplane respond beyond a certain  
>rate: namely, the rate that limits stress on the airframe to... 2.5G.

This is indeed a problem. There are situations where the crew may elect to damage the airframe in return for avoiding a worse alternative. The protection system will not let them do this. It's not clear whether we'll lose more people from not having such a system or because of it. One point worth considering is that second generation fly-by-wire systems for fighters are now being designed to allow maneuvering beyond critical alpha as the disadvantages (high drag, loss of airspeed, structural risk) may allow the pilot to shoot first and thus survive.

[re: the 747 loss of control incident]

>Airbus, not surprisingly, responds that an A320 never would have [entered the  
>dive] in the first place.

This contention may be incorrect. The flight control laws prevent a pilot from deliberately maneuvering the aircraft to a control departure, but they don't prevent one from occurring under all conditions.

As part of a previous job, I occasionally flew an advanced cockpit flight simulator. I was curious as to the flight limits, and found them rather rapidly. The flight control laws would not allow me to roll the airplane beyond 70 degrees of bank. It seemed obvious to me that an aerodynamic departure could result in a maneuver that would exceed the control law limits. I brought the aircraft to the limiting angle of attack, then reduced thrust on one engine to idle. The resulting asymmetric thrust produced a rolling moment that caused the aircraft to exceed the control limits by a considerable margin. This is virtually the same situation as occurred on the 747 mentioned above, and could conceivably occur on an Airbus aircraft with control-law limits.

One more anecdote: Several years ago an Air Florida 737 crashed into the

Potomac River. One of the contributing causes was faulty engine power indication. The crew believed that maximum power was being applied, but their indications showed considerably more power was being generated than was actually being produced. There was nothing preventing them from advancing the power levels beyond the "max power" setting other than training that predisposed them to not do this. It is now regarded as correct procedure to exceed such limits in an emergency if doing so might save the aircraft. You can always replace the engines after the emergency landing. If you would have crashed without such power application, the engines (among other things) would be lost anyway. If they fail from excessive power application, well, you were going to crash anyway. This is, after all, an effort of last resort.

It is a classic error to design systems to handle the majority of cases correctly but omit the handling of limit cases. Advanced systems are intended to increase safety and efficiency. It would be an error to design-out application of control in limit cases that might be necessary to save lives.

---

### **✈ Automobile Electronic Performance management**

*"Pete Lucas, NERC Swindon UK." <PJML@ibma.nerc-wallingford.ac.uk>  
Fri, 14 Jul 89 10:23:11 BST*

There has recently been some considerable discussion of the potential risks associated with 'fly by wire' systems in airplanes, and the way in which the electronics prevent excursions outside a pre-defined 'performance envelope'. This sort of thing is not only found in planes - there are now on the market (in the United Kingdom at least, not sure about the States) quite a number of high performance automobiles which do much the same thing.

Examples are: electronic monitoring of turbocharger boost/charge temperature to prevent detonation, monitoring of engine speed (prevents overspeed), control of auto transmissions (to prevent shifts to low gears at high road speeds) etc.

Most of these limitations are done to prevent possibly hazardous and damaging operation of the vehicle, others are done to comply with the national or regional restrictions on exhaust emissions, or to adapt to the local fuel octane availability. They do, in many cases, mean that the vehicle is also operated well within its design limitations, hence helping to reduce manufacturers warranty claims.

There are several organisations in Europe which have, by devious means, gained access to the control programs of these microprocessors (either by disassembling, or by blatant and unashamed bribery of the software writers) and are thus able to modify the software and produce what they then sell as 'Superchips' that, for a couple of hundred pounds and ten minutes effort with a chip-puller, can transform the performance of an already rapid car - examples given in UK literature are as follows::

Sierra/Merkur Cosworth - 388 brake horsepower  
Volvo turbos - 280 brake horsepower  
Mazda 323 - 180 brake horsepower

Nissan 300ZX - 370 brake horsepower  
SAAB turbos - 280 brake horsepower.

Now apart from the potential hazards of improperly programmed microprocessors leading to the destruction of engines/transmissions due to excessive stress that the manufacturer/designer did not foresee, i wonder about the legal position of the car should you be involved in an accident. Cars in Europe have to be 'Type approved', that is to say, there are national testing authorities who oversee the safety of production cars and prevent the sale or import of those vehicles that fail to reach certain standards. Any modifications to a type-approved vehicle should strictly only incorporate parts that have been themselves type-approved. In this context, 'software' is a rather tenuous 'part', again lawyers lagging decades behind technology..... There are, as far as i am aware, no provisions for policing the status of on-board software, nor to prevent its alteration. Since the changes are visually undetectable (who walks round their local friendly used car lot with a signature analyser and an EPROM blower in their pocket?) it would be very hard to spot, either by the licensing authorities, or the insurers who may be asked to meet claims resulting from accidents.

Don't any of you think i am against the enhancement of performance of vehicles - i want my 70-90 acceleration times to be as short as is humanly possible (and anyone who has driven the motorway network here will agree on that!), its just that i can foresee potential problems in the future (like what is the risk if you sell such a modified vehicle and fail to disclose the modifications and the purchaser then smashes himself up - can he sue you for failing to tell him about the changes???)

Pete Lucas. PHONE: +44 793 411665

JANET: PJML@UK.AC.NERC-WALLINGFORD.IBMA EARN : PJML%UK.AC.NWL.IA@UKACRL



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 9: Issue 6

Monday 17 July 1989

## Contents

- [Mitnick sentenced as an addict](#)  
[Rodney Hoffman](#)
- [Long addresses confuse bank's computer](#)  
[Paul Leyland](#)
- [Town Hall's computer snags trouble old age pensioners](#)  
[Olivier Crepin-Leblond](#)
- [Re: Automobile Electronic Performance Management](#)  
[Charles Rader](#)
- [Re: UK Defence Software Standard, non-determinism, recursion and armageddon](#)  
[Victor Yodaiken](#)  
[anonymous via Tim Shimeall](#)  
[Bob Estell](#)  
[Martin Minow](#)
- [Telephone technicians tapping into other phone lines](#)  
[Olivier Crepin-Leblond](#)
- [Re: New Yorker Article on "radiation" risks](#)  
[Gordon Hester](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✉ Mitnick sentenced as an addict

*Rodney Hoffman <Hoffman.ElSegundo@Xerox.com>  
18 Jul 89 08:49:34 PDT (Tuesday)*

Kevin Mitnick is the hacker once called "as dangerous with a keyboard as a bank robber with a gun." (See [RISKS 7.95](#), 8.1, 8.3, 8.43, 8.65, 8.70, and 8.76.)

His first plea bargain was rejected by U.S. District Judge Mariana R. Pfaelzer as too lenient. He subsequently reached a new agreement, with no agreed-upon prison sentence, in which pleaded guilty to stealing a DEC security program and illegal possession of 16 long-distance telephone codes belonging to MCI Telecommunications Corp. If convicted of all counts, Mitnick faced a maximum sentence of 20 years and a fine of \$750,000.

According to a story by Henry Weinstein in the 18 July 1989 'Los Angeles Times', Judge Pfaelzer said Monday that she will sentence Mitnick to a year in a rehabilitation center, where he can be treated for his "addiction." It is believed to be the first time a person indicted for a computer hacking - related crime will be treated as an addict.

Harriet Rossetto, the director of the rehabilitation center said that Mitnick would benefit from the program. She said that Mitnick's "hacking gives a sense of self-esteem he doesn't get in the real world.... This is a new and growing addiction . There was no greed involved. There was no sabotage involved.... He's like a kid playing Dungeons and Dragons."

Asst. U.S. Attorney James R. Asperger told Pfaelzer that he was amenable to the rehabilitation plan, in part because Mitnick has cooperated extensively with the government in its case against DiCicco, Mitnick's one-time friend who turned him in. Asperger said that Mitnick had turned out to be considerably less harmful than the government had originally thought, particularly since he not broken into DEC's computer system out of malice or to make money.

Judge Pfaelzer said she will rule today on whether Mitnick should serve any additional prison time, beyond the seven months he has so far spent in federal custody. DiCicco still faces one federal charge of illegally transporting a stolen program (!).

---

### **⚡ Long addresses confuse bank's computer**

*Paul Leyland <pcl@robots.oxford.ac.uk>*

*Tue, 18 Jul 89 15:04:00 BST*

In today's copy of "The Times" (of London), there is a sketchy description of problems which arose from the country's first flotation on the stock exchange of a building society. [For the benefit of non-UK readers, a "building society" is an organisation whose purpose is to collect deposits from its members; pay them interest on the money; provide mortgages secured on property and collect the interest due on the loan. Sort of like a bank, but more restricted in what it can and cannot do. I forget the name of the US analogue.] It is only recently that building societies have become allowed to raise finance by public flotation and there has been much heated debate about the morality of the operation. In particular, people with accounts at the Abbey National Building Society were guaranteed cheap shares at the flotation. Lloyds Bank, who handled the flotation, are the third largest bank in the UK -- certainly *\*not\** a tin-pot outfit.

The following is from "The Times", Tuesday 18 July 1989.

Compensation offer for Abbey delay.

Lloyds Bank Registrars are offering to compensate 120,000 Abbey shareholders whose share certificates and return cheques have been held up in the post. This group suffered because their addresses were jumbled up by the computer,

which was unable to read addresses with more than five lines. It was originally thought no more than 10,000 people were affected by this error, but it emerged last night that 120,000 people are involved.

The Abbey National has already said it will back-date -- to Wednesday, July 12 -- delayed cheques that are returning sums over-paid for shares, if they are paid into an Abbey National Account. But many would-be share owners say they have borrowed large sums to buy shares and the delay in returning cheques is costing them missed interest and also interest on loans. All Abbey members who applied for more than 600 shares at 130p were scaled down to 775 shares. As a result, some people who made massive applications are awaiting the return of hefty cheques.

Mr Charles Wootton, a member of the Abbey National Protest Group, who applied for 100,000 shares at a cost of \pounds 130,000 [[approximately US\$ 200k]], said that he had lost interest on the money taken out of a higher interest account. "They have had our money for an awfully long time", he said.

It is unprecedented for Lloyds Bank Registrars to offer compensation for a bungled share allocation, but a Lloyds spokesman said: "The scale of the thing was unprecedented".

Lloyds is writing to the 120,000 people whose addresses were jumbled by the computer asking if they had any special problems. Each compensation claim will be dealt with individually on its own merits. Lloyds will want proof that a loan was outstanding against the cash used to apply for shares.

There is no question of any compensation for the slide in the Abbey share price from a brief high on the first day's trading of 161p to 145p yesterday.

[I wonder what 120,000 personal letters and investigations are going to cost....

Paul Leyland]

---

### **✂ Town Hall's computer snags trouble old age pensioners**

<ZDEE699@elm.cc.kcl.ac.uk>

Mon, 17 JUL 89 19:35:08 GMT

TOWN HALL'S COMPUTER SNAGS TROUBLE OAP'S [OCL. Old Age Pensioners]  
[From the Kensington and Chelsea Times, a [very] local newspaper]

Many private tenants in Kensington & Chelsea are living in poverty as a result of the council's inability to cope with its housing benefit workload, claims Kensington & Chelsea "Put for the Elderly".

"Everyone who claims housing benefit must fill-in a new benefic application form every year", says the group. "If the application is not received by the Housing Benefit Office within four weeks, a reminder is sent-out and if this is ignored, housing benefit is stopped."

"However, in Kensington & Chelsea, payment is bein gstopped because council

staff are unable to feed the information into the computer quickly enough. There is a huge backing of such information waiting to be logged into the computer's memory."

It is alleged that Housing Benefit payments have been stopped for "hundreds" of people while their re-applications wait to be dealt-with. "It can be weeks before payments resume."

"This is particularly hard on senior citizens who are known as society's most conscientious bill-payers. Many older people will go without, rather than get into debt."

The Royal Borough Council admits that there is a problem, and expresses its intention to remedy the situation. "There has been a backlog but we hope to have the situation under control by the end of the month".

A report by the Royal Borough Council's Benefit Working Party analyses the reasons for the build-up of work in the benefit's division:

"The computer is not powerful enough to cope with the heavy demands that are being placed upon it. Consequently, the officers are struggling to process assessments sufficiently quickly to match incoming work.

There have been a number of computer crashes in recent months, resulting in a lot of 'down' time."

The report continues:

"The computer software developed a fault which resulted in our inability to produce the weekly notification letters that have to be sent to the claimants. This continued for some eight weeks during March and April this year, and meant that when the fault was rectified, there was a large backlog of letters produced.

"Statutory case reviews have brought about large numbers of claims being processed. Between April 1988 and March 1989 it was not possible to undertake these reviews because of computer difficulties.

Olivier Crepin-Leblond, Computer Systems & Electronics,  
Electrical & Electronics Engineering, King's College London, England

---

## **Re: Automobile Electronic Performance Management**

*Charles Rader <cmr@carp.uucp>*

*Mon Jul 17 01:13:23 1989*

I have three anecdotes related to this topic.

First:

A personal experience several years ago suggests General Motors enforces the "performance envelope" on its cars.

While descending a steep mountain grade in a 1981 Chevrolet Cavalier using engine braking to control speed, the automatic transmission shifted into second gear even though the gearshift lever remained locked in first gear.

The engine speed was near the "yellow line" when it shifted, so I suspect this was a feature intended to prevent engine damage. The behavior was reproducible.

I had left GM for my present job and didn't ask my GM contacts about it.

In this case, I had good brakes. What if the brakes had failed?

Second:

I heard of an incident several years ago where electronic component failure caused a vehicle to exceed the design envelope. During quality assurance testing at an assembly plant (on dynamometer rollers), a cruise control component failure caused wide-open throttle and loss of brakes. The technician cut the ignition before the engine destroyed itself.

The design problem was apparently fixed before it recurred.

I wasn't present when this happened so I'd rather not name the company or plant, but the story was reported by individuals I trust to have the facts.

Third:

Bootleg PROMs exist in North America, too. Some auto company engineers have mentioned programming them for personal use.

Charles Rader, Systems Manager, Univ. of Detroit Computer Services, 313-927-1349

---

## **✶ non-determinism, recursion and armageddon**

*victor yodaiken <yodaiken%ccs2@cs.umass.edu>*

*Sat, 15 Jul 89 20:14:52 EDT*

I'm puzzled as to what Nancy Leveson means when she uses the term "non-deterministic". Leveson seems to be arguing that any program with hidden side effects is non-deterministic. The dangerous techniques she mentions, distributed processing, interrupts, dynamic memory allocation, recursion, have in common an effect on program state that are not exposed in the program text. That is, to verify a recursive subroutine written in Pascal, one needs to also verify the stack management methods of the compiler, and the memory limits of the machine. As the entire Hoare/Floyd etc. approach to verification is based on reasoning about program text, these techniques can pose problems for the verification method. I have 4 critiques of this analysis (3 technical, 1 horrified):

1. The inability of a verification system to handle a programming technique does not imply that the technique is at fault. The verification method might just be too weak.
2. Even if we give up all these very useful techniques, there are still hidden side effects in programs, especially real-time programs, which cannot be deduced from the program text. Subroutine call stacks may overflow, even without recursion, and access to statically allocated memory is not necessarily uniform (suppose that  $A[i]$  is compiled to a single machine operation for  $i < 256$  and requires segments and some other mess for  $i > 255$ ).
3. Hidden side effects  $\neq$  non-deterministic. A non-deterministic

system can react to one input in more than one way --- there is no way, even in principle, to deduce output from input. But, even poorly written programs are deterministic --- the same environment will cause the same execution trace. Am I confused here, or is non-determinism being used in some other way.

4. If X (name your favorite agency or company) is going to have the gall to develop programs that might kill millions of people when they fail, e.g. nuclear reactor control programs or missile control programs, then X should at least have the decency to hire the best programmers for the job and have the entire system checked out by technically competent experts ( at least several independant certifications would also seem reasonable)

Leveson seems to be saying that since military programmers, and the people who certify military programs are sometimes bad, we should force them to use very simple programming methods. The following quote (from Leveson) gave me the shakes.

>Although I have great confidence that David

>Parnas or Edsger Dijkstra could use ANY techniques with great skill, I

>have less confidence that this is true for all the programmers writing

>military software.

...

>Remember, we are talking about a potential nuclear

>armageddon here and with certifiers who may be no more knowledgeable

>than the programmers.

The rational approach here is to send a check to SANE (CND for Brits), not to try to forbid recursion.

---

## **✉ Re: UK Defence Software Standard**

*Tim Shimeall x2509 <shimeall@cs.nps.navy.mil>*

*Mon, 17 Jul 89 12:17:17 PDT*

[Forwarder's Note: The following is a statement by a close friend, who wishes to remain anonymous but asked me to forward this statement to risks. His comments do not apply to his current employer, and any identification of him might generate misunderstandings. My friend does read RISKS, and any personal replies may be addressed to me and I will relay them.

Tim]

I have some experience in working in a RISKy (non-aerospace, non-military) branch of the software industry, and for this reason I have read with interest and increasing concern the debate in risks over UK Defence Software Standard.

My concerns are not so much with the standard itself, as with the academic viewpoint reflected in the arguments stated there and their broader implications for those of us who worry about software quality in the real day-to-day world. The basis of my concern is the assumption that either all software engineers working on RISKy projects would understand well such concepts as recursion, multi-tasking, and dynamic memory allocation, or that

only people with these qualifications would be assigned to work on such projects.

I do not have the academic credentials of Professor Parnas, but I do have a number of years of experience in QA and Test of software in the real world. I have been responsible for the evaluation of well over 100 pieces of software. Only a small fraction of the engineers working these projects understood well the nuances of the methods listed above.

Most of them have never heard of Dijkstra, and of the few who have, none to my reasonably accurate knowledge have ever read anything he has written. Many of them have only high school diplomas or AA degrees in electronics. The point I am trying to make here is that, rightly or wrongly, the real world does not reflect the academic one in these areas. In my experience, the aerospace companies generally have much better educated software engineers, but even there, many of them have not been to school in over 20 years.

For this reason, I think that instructing or allowing the average software engineer in industry to use some of these techniques in life-critical applications is a lot like putting a loaded 45 into the hands of a child. Thus, in my humble and very pragmatic opinion, statements by Professor Parnas such as:

- > Nor, would I agree that non-determinism is bad. Non-determinism has been
- > demonstrated by Dijkstra (and much earlier by Robert Floyd) to allow
- > programs that are much more easily verified than some deterministic ones.
  
- > I believe that organisations such as MoD would be better advised
- > to introduce regulations requiring the use of certain good
- > programming techniques, requiring the use of highly qualified
- > people, requiring systematic, formal, and detailed documentation,
- > requiring thorough inspection, requiring thorough testing, etc.
- > than to introduce regulations forbidding out the use of perfectly
- > reasonable techniques.

To be very naive.

Professor Parnas has experience with aerospace, but in many other software industries with life-critical applications things are much worse. These industries would hire people with the kind of qualifications he discusses were they available. The fact of the matter is that the people are simply not there. Thus it seems to me that the best approach to take is to develop standards designed to work with the present environment, rather than try to build standards designed to work in the environment that should be.

Comments to me may be made via Dr. Shimeall. Thank you for considering the views of one eminently less qualified on academic grounds. These opinions are my own, and are not the opinions of either Dr. Shimeall or my present or previous employers, both of whom would be very upset to find that I had expressed them in public.

---

 **polling vs. interrupts: some perspective'**

"FIDLER::ESTELL" <estell%fidler.decnet@nwc.navy.mil>

17 Jul 89 15:31:00 PDT

A comment on the "interrupt vs. polling" debate, if I may.  
I submit that which is better is very much a matter of perspective; and further, that the perspective is scenario or (environment) dependent.

If one takes the point of view of the "operating system kernel" looking from inside ONE processor, out to the world, AND \*IF\* that world is simple and small, and \*docile\*, then polling is very straightforward. Using Prof. Einstein's rule [... simple as possible, but no more ...] perhaps then polling is to be preferred, in those cases.

However, as the world [system] grows larger, more complex, and less well behaved, polling becomes enormously more complex. Not the least of the problems is, what algorithms does one use, when and how, to handle emergencies [call them "interrupts" is you wish] that occur randomly, in such a way that the priority of handling them MUST change?

Example: In a tactical combat system, implemented on several processors, distributed among several sites (with at least 2 but at most say 7 processors per site), a normal goal is to share messages in real time; under fire, however, most especially when one or more processors at any given site may suffer damage, priority swiftly shifts towards defending oneself; i.e., the "data link" module becomes somewhat less important than the "track and shoot" modules. However, since coordinated fire is often more effective than "self defense" fire, some link should be maintained.

Perhaps we can learn from successful (?) systems significantly more complex than those we seek to build; e.g., ourselves. SOME of our sensors usually do polling; e.g., our eyes; occasionally we get interrupted by flashes of light; but more often, we scan the scene. However, our ears most often operate on interrupts. And our brains use adequate algorithms to process and correlate those diverse data.

Bob

---

### **✶ re: Non-deterministic interrupt handling**

*Repent! Godot is coming soon! Repent!* <minow@bolt.enet.dec.com>

17 Jul 89 21:34

In [risks 9.5](#), Dave Parnas writes:

>The non-determinism associated with interrupt handling comes from the unknown  
>timing of the external events and is not affected by the replacement of  
>interrupts with polling.

Much of the variation in interrupt handling comes from other operating system processing, such as (in modern computer systems) page-faulting and job/swap/memory management. Also, in very modern systems, the hardware instruction and data cache mechanisms introduce additional variation.

This is true in all aspects of interrupt processing: not just in the response time as measured in the user's program.



The answer from the French Telecom, is to ask for itemised bills.  
And believe me, it comes as a shock when your bill says that you've been  
calling St. Bartholomew and you don't even know where it is !

Olivier Crepin-Leblond, Computer Systems & Electronics,  
Electrical & Electronic Engineering, King's College London, UK

---

**✉ Re: New Yorker Article on "radiation" risks**

*Gordon Hester <gh0t+@andrew.cmu.edu>  
Fri, 30 Jun 89 20:45:47 -0400 (EDT)*

There have been a couple of postings about the series of New Yorker articles by Paul Brodeur recently. I happen to work (as a researcher) in the area of electric and magnetic fields (EMF) risks. (The use of the term "radiation" by Brodeur is a complete misnomer, by the way - he's talking about fields.) I'm not a health effects researcher - my field is risk communication and public policies for risk management. Anyway, I would like to pass along a couple of comments.

The first comment is that no one really knows at this point whether there are risks (i.e., adverse health effects) from EMF. Scientific investigation in this field is very complex and difficult. There have been a lot of flawed studies (with both positive and negative results.) There are clearly demonstrated biological effects, but no one knows whether these cause health effects. (The alternative is that the body adjusts to the biological effects, or that they are somehow unimportant.) There is certainly reason for sufficient concern to continue to fund research, although money has been hard to come by in this area as a rule. A little more support seems to be forthcoming recently.

Second, Brodeur's descriptions of the ways scientists have supposedly "cooked" their data to suit the preferences of funding sources are, in large part, B.S. Not that none of this has ever occurred - it has, and on both sides of the issue. But it is the exception, not the rule by any means. There are some good scientists working in this area, and they are men and women of high integrity. Their's are the results worth taking seriously, and fortunately they are getting the lion's share of the funding these days.

The third thing, in case it's not obvious to anyone who read the articles, is that Brodeur is anything but an unbiased observer. He has reached his own conclusions, and is seemingly out to convince people no matter what it requires saying. Notice that, for example, according to him it's only the scientists who come up with negative results (on health effects) who are cooking their data. I would caution net readers against relying on these articles as your sole source of information if you have a serious interest in this topic. If you do, send me email if you want recommendations for other sources.)

BTW, despite my reservations about the Brodeur articles, the most recent posting to the net on this topic (sorry, I don't have the name handy) did pick out some interesting points from them.

gordon hester, carnegie mellon u., department of engineering and public policy

pittsburgh, pa 15213

gh0t+@andrew.cmu.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 9: Issue 7**

**Wednesday 19 July 1989**

## Contents

- [Re: Gordon Hester on Paul Brodeur \(Radiation\)](#)  
[Jan Wolitzky](#)
- [Computers consume wine](#)  
[Hugh Davies](#)
- [Mitnick sentence](#)  
[Rodney Hoffman](#)
- [Re: DARPA contract: use AI to select targets during nuclear war](#)  
[Lee Naish](#)
- [Reliance on technology](#)  
[Jake Livni](#)
- [Summer slowdown for RISKS](#)  
[PGN](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **✉ Re: Gordon Hester on Paul Brodeur**

<[wolit@mhuxd.att.com](mailto:wolit@mhuxd.att.com)>  
Wed, 19 Jul 89 09:42 EDT

I have some real problems with Gordon Hester's recent attack on Paul Brodeur's series of articles in The New Yorker on the hazards of electromagnetic radiation.

Hester writes:

The use of the term "radiation" by Brodeur is a complete misnomer, by the way - he's talking about fields.

Anyone who's taken a high school physics course knows that this is bull -- electromagnetic radiation IS radiation, whether it's ELF 60 Hz radiation from power lines, or X-rays from nuclear reactions. The only difference is wavelength (or frequency, or energy, which are different ways of expressing the same thing). Calling them "fields," and avoiding the term "radiation," is an attempt to mislead the unwary, to put some good "spin" on the story. Sure, you

can discuss the electric and magnetic fields separately, but it is NOT a misnomer by any means to refer to the subject as radiation.

Hester's piece was the second I read today from CMU. The first was a booklet by M. Granger Morgan, also of the Dept. of Engineering & Public Policy, entitled, "Electric and Magnetic Fields from 60 Hertz Electric Power: What do we know about possible health risks?" The booklet was mentioned in the July issue of the IEEE Spectrum, and is for sale by CMU for \$3.

The booklet also goes to great pains never to use the word "radiation" in connection with electric power lines, except to say that it's not like X-rays or other forms of "ionizing radiation" (quotes in the original). It also tries to discount epidemiological data that establishes a correlation between ELF radiation and cancers and birth defects, by saying that just because a rooster crows in the morning when the temperature is rising doesn't mean that the rooster CAUSED the temperature to rise.

There seems to be a concerted effort on the part of the Dept. of Engineering and Public Policy at CMU to lobby the public that there's nothing to get excited about here, that scientists don't all agree on the interpretation of the data and that therefore we should follow a "prudent" course (they use that word a lot), by which they mean no government regulation at all, just maybe you should put your electric blanket back on the shelf in the closet.

To understand why an academic institution would go to such lengths to try to dampen public interest in the health risks of ELF radiation, I had to read the fine print in the front of the booklet, where I discovered that the research was supported, and the production costs of the booklet paid for, by the Electric Power Research Institute, a lobbying arm of the electric power industry in this country.

Jan Wolitzky, AT&T Bell Labs, Murray Hill, NJ; 201 582-2998; mhuxd!wolit  
(Affiliation given for identification purposes only)

---

### **✶ Computers consume wine**

<"hugh\_davies.WGC1RX"@Xerox.COM>  
19 Jul 89 00:24:07 PDT (Wednesday)

Quoted, from the 18th July edition of the London "Daily Telegraph".

Customs 'lose' 35.6 million wine bottles

Customs officials admitted yesterday that their computers had "lost" 35,600,000 bottles of wine, destroying the reliability of figures on how much wine Britons are drinking. "We never dreamed the error by Customs could be so enormous," said Mr. Alastair Eadie, chairman of the Wine and Spirit Association, which queried returns dating back to the start of last year.

It emerges that the computers developed such a liking for wine that they kept millions of bottles to themselves. Figures were entered correctly, but not released when needed to compile statistics. All wines, apart from small

quantities made at home by enthusiasts as a hobby, have to go into bonded warehouses so duty can be charged on them before they are sold. That is why records are kept on computer by the tax collectors.

At the start of last year, Customs and Excise updated its computer methods and something went wrong. "All the information went in but not all of it came out again," it was stated. It did not mean that vast quantities of wine escaped duty. That was correctly paid whenever supplies were drawn from bond. It meant sales were grossly understated when official returns were issued at the end of each month. The trade relies on these figures for a nationwide picture of how sales are going.

Wine merchants became suspicious as official figures showed sales declining when shop returns suggested otherwise. And the monthly statistics started to suffer delays, being issued later and later. "What's gone wrong?" the Association asked. Now they have the answer.

The correction means that wine drinking in Britain rose by more than 3% instead of declining 1% as originally reported by Customs. "This is splendid news," said Mr. Eadie. "And the provisional data for the first quarter of 1989 shows a rise of nearly 5 and-a-half percent compared with the first quarter of last year." Sales of sparkling wines, which includes champagne, alone increased by 22% "Three months is scarcely enough to suggest a trend for 1989 as a whole but they make a fine start." Mr. Eadie said. "Wine trade prospects have definitely brightened considerably."

---

✂ **Mitnick sentence (See [RISKS 9.6](#) for background.)**

*Rodney Hoffman <Hoffman.ElSegundo@Xerox.com>  
19 Jul 89 07:36:37 PDT (Wednesday)*

Confessed computer hacker Kevin Mitnick was sentenced Tuesday to 1 year in prison, followed by three years of "supervised release," the first six months of which will be spent in a residential psychological counseling program, according to an article by Henry Weinstein in the 'Los Angeles Times' 19 July 1989. The 7.5 months Mitnick has spent in custody while charges were pending against him will be credited against his one-year prison sentence.

Prosecutor Asst. U.S. Attorney James R. Asperger said, "We think it's a very fair sentence. The sentence shows computer hacking is serious business that can result in jail time."

---

✂ **Re: DARPA contract: use AI to select targets during nuclear war**

*Lee Naish <munnar!munmurra.mu.oz.au!lee@uunet.UU.NET>  
Mon, 17 Jul 89 21:09:32 EST*

> o Enhanced deterrence through the ability to hit mobile targets.

Unless the Soviets have developed mobile cities this is not deterrence. This is "counterforce". This is "first strike". One of the RISKS of developing

such technology is that in a potential East-West conflict situation the opposing forces might implement a "use them or lose them" strategy with respect to their delivery vehicles (as they would say in the DoD).

Lee Naish (lee@cs.mu.oz.au)

---

### **✂ Reliance on technology**

Jake Livni <JAKE%Irving@VX1.GBA.NYU.EDU>

Tue 18 Jul 89 17:52:12-EDT

There is a RISK in *\*BECOMING DEPENDENT\** on technology, instead of merely using it for efficiency and convenience. (Imagine not having ATMs anymore and having to run to the bank before it closes.)

From RISKS-DIGEST 9.4:

- > Unspecified hardware problems caused 104 brief failures in a new ...
- > An emergency technical crew was FLOWN IN [emphasis mine] from New Jersey
- > and worked all night Monday to correct the problem.

Wouldn't it have been funny if we REALLY NEEDED the TRACON working in order to fly in to California? Then the emergency crew might have had to take AMTRAK...

Jake Livni

---

### **✂ Summer slowdown for RISKS**

Peter G. Neumann <Neumann@KL.SRI.COM>

Wed, 19 Jul 89 22:16:55 PDT

I will have very limited time and net access for the next 3.5 weeks (but only a day or two of vacation). If this is a period when mishaps and disasters cry out for RISKS discussions, send in your contributions anyway and I'll get to them whenever possible. 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 9: Issue 8**

**Friday 28 July 1989**

## Contents

- [Returning before departing on airline reservation systems](#)  
[Gary McClelland](#)
- [Sun security problem: restore](#)  
[J. Paul Holbrook](#)
- [Computer condom?](#)  
[Jeff Stout](#)
- [Robert Tappan Morris indicted](#)  
[Steve Den Beste](#)
- [Re: UK Defence Software Standard](#)  
[Mark Moraes](#)  
[Douglas W. Jones](#)
- [Polling vs. interrupts](#)  
[Douglas W. Jones](#)
- [Software Engineering Models \(John J.G.\) Mainwaring](#)
- [Single Point of Failure for Internet Management](#)  
[Kee Hinckley](#)
- [DARPA contract & AI for moving targets](#)  
[Bob Estell](#)
- [Two-Word Last Names and Other Amusing Database Stories](#)  
[Gary McClelland](#)
- [Credit card issuers invade cardholders' privacy](#)  
[Andrew Klossner](#)
- [Re: windowless cockpits](#)  
[Andrew Klossner](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✂ Returning before departing on airline reservation systems

"Gary McClelland" <[gmcclella@clipr.colorado.edu](mailto:gmcclella@clipr.colorado.edu)>  
25 Jul 89 15:23:00 MDT

From the "Rumor Roundup" column in DIGITAL REVIEW (trade newspaper that tracks DEC doings) of 17 July 1989:

My DEC friends tell me that DEC employees now have a special way of traveling back in time. It seems that a memo on the internal electronic bulletin board goes on at great length about how to take advantage of a loophole in the rules governing domestic discount airfares. By booking the return flight as the departing flight, and the departing flight as the return flight, the airline computer system thinks the traveler is staying over the weekend. Apparently, the reservations program does not understand that people have to leave before they can return.

Gary McClelland, gmcclella@clipr.colorado.edu

---

### **✖ Sun security problem: restore**

<cert@SEI.CMU.EDU>

Wed, 26 Jul 89 09:20:48 EDT

A security hole has been found in SunOS restore. This problem affects SunOS 4.0, 4.0.1, and 4.0.3 systems. It does not appear in SunOS 3.5. The problem occurs because restore is setuid to root. Without going into details, is sufficient to say that this is a serious hole. All SunOS 4.0 installations should install this workaround. Note that a user does need to have an existing account to exploit this hole.

There are two workarounds that will fix the problem. The first is slightly more secure but has some side-effects.

1) Make restore non-setuid by becoming root and doing a  
chmod 750 /usr/etc/restore

This makes restore non-setuid and unreadable and unexecutable by ordinary users.

Making restore non-setuid affects the restore command using a remote tape drive. You will no longer be able to run a restore from another machine as an ordinary user; instead, you'll have to be root to do so. (The reason for this is that the remote tape drive daemon on the machine with the tape drive expects a request on a TCP privileged port. Under SunOS, you can't get a privileged port unless you are root. By making restore non-setuid, when you run restore and request a remote tape drive, restore won't be able to get a privileged port, so the remote tape drive daemon won't talk to it.)

2) If you do need to have some users run restore from remote tape drives without being root, you can use the following workaround.

```
cd /usr/etc
chgrp operator restore
chmod 4550 restore
```

This allows the use of restore by some trusted group. In this case,

we used the group 'operator', but you may substitute any other group that you trust with access to the tape drive. Thus, restore is still setuid and vulnerable, but only to the people in the trusted group.

The 4550 makes restore readable and executable by the group you specified, and unreadable by everyone else.

Sun knows about this problem (Sun Bug 1019265) and will put in a more permanent fix in a future release of SunOS.

J. Paul Holbrook, Computer Emergency Response Team,  
Internet: <cert@SEI.CMU.EDU> (412) 268-7090 (24 hour hotline)

---

### **✂ Computer condom?**

<jstout@atc.boeing.com>  
Mon, 24 Jul 89 10:59:30 PDT

[From the Seattle Weekly, 5/3/89]

#### PUT A CONDOM ON YOUR COMPUTER

Every worry that your computer might be hanging out in a network where it will pick up some disgusting virus? Empirical Research Systems of Tacoma suggests you supply it with one of their "computer condoms". This high-tech prophylactic is a combination of hardware and software embodied in a controller card that simply replaces the one already in the machine. Rick Cummings, the company's president, says the system "stops all viruses" by monitoring the user network, the keyboard, and the program in use. He notes that the system is programmable to alter the parameters of its control on any given machine, but he guarantees that, "when programmed to your requirements, it will not allow viruses to enter."

The technology was developed through successful efforts to protect a group of European banks from the massive virus that penetrated European computer networks last autumn. "Naturally these became our first orders," Cummings says. He has since picked up an additional 2500 firm orders in Europe, with 5000 more contingent on inspection of the product. In the United States, the product has been reviewed by Boeing Computer Services and computer technicians at the UW. It will be on the domestic market "early next autumn at a cost of under \$1000," Cummings says.

[An untapped market for LaTeX? --JCS]

Jeff Stout Electrons: jstout@atc.boeing.com, uw-beaver!bcsaic!jstout  
Molecules: Advanced Technology Center, Boeing Computer Services,  
M/S 7L-64, P.O.Box 24346, Seattle, WA 98124-0346

---

### **✂ Robert Tappan Morris indicted**

<denbeste@BBN.COM>

Thu, 27 Jul 89 10:44:56 -0400

The 7/27/89 Boston Herald reports that Robert T. Morris has been indicted on a single felony count of accessing without authorization at least six (!!) university and military computers. He therefore becomes the first person to be charged under the "Computer Fraud and Abuse act of 1986", a dubious honor at best. If convicted he faces a possible prison sentence of 5 years and a possible \$250,000 fine.

---

### **✉ Re: UK Defence Software Standard**

Mark Moraes <moraes@ai.toronto.edu>

Thu, 20 Jul 89 10:18:58 EDT

You precisely underline the risk involved - that the software engineers working on life-critical might not be trained in "modern software engineering".

One does not have to be an academic computer scientist to understand recursion, dynamic memory allocation, multi-tasking, and interrupts. One does not have to be an academic computer scientist to use them, or to decide not to use them.

However, decisions to use or not use such techniques must be informed, and made from knowledge, not ignorance. Turning one's back on new techniques because they are risky in the hands of untrained people is not the answer - training them in the new techniques is.

Yes, training people in software engineering is an expensive business - it also takes time, and is an ongoing process. But if someone involved in RISKy projects is not a top-flight software engineer, isn't that a serious risk to the project? And to the lives that may depend on it?

---

### **✉ Re: UK Defence Software Standard**

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

Fri, 21 Jul 89 10:03:16 CDT

The terms software engineering and software engineer have clearly gotten completely out of control if people with AA degrees or less are calling themselves software engineers. It is my understanding that the ABET takes a very strong stand on who should be allowed to call themselves an engineer. If I remember correctly, they say that the term should only be applied to those who have one of the following qualifications:

- 1) People who have passed a state professional engineering examination.
- 2) People who have graduated from an accredited 4-year engineering program.

### 3) People who have graduate degrees.

In the past, I have had a fairly negative feeling towards this strict rule. As a professor of computer science in the liberal arts college of a large university, I've always had the feeling that it discriminated against graduates of my program in favor of graduates of similar programs that happen (usually for historical reasons) to be in engineering colleges.

I feel strongly enough about the misapplication of the term software engineer that, if things continue to develop the way they are currently developing, I would even be willing to urge state regulation of the use of the designation.

Consider an analogy: The people who design the power distribution system for a power plant are electrical engineers. They have college degrees in electrical engineering, they are usually fairly senior, and they usually have state professional engineering certificates. The people who build the power distribution system are electricians working under the supervision of an electrical engineer. They may have AA degrees in engineering technology, and they have passed a state or local electricians examination.

I do not object to someone with an AA degree in software technology helping to write the software to control that power plant, but I do object to their billing themselves as a software engineer, and I do object if the power company puts them in charge of the design of such software. This appears to be precisely what is happening today.

Douglas W. Jones, University of Iowa, jones@herky.cs.uiowa.edu

---

### polling vs. interrupts

*Douglas W. Jones <jones@pyrite.cs.uiowa.edu>*

*Fri, 21 Jul 89 11:16:23 CDT*

I have enjoyed the recent arguments about polling and interrupts that were kindled by the UK defense software standards debate, but I have found them to be incomplete.

I have written real-time software, I have worked on the design of real-time multiprocessors, and this summer, I have even spent far too many hours counting cycles, but I also like interrupts.

When I was involved with the Modcomp User's Group, and again, when I worked for Rockwell International, I met many strong advocates of the view taken by the UK software standards. Most of them were older programmers who hadn't heard of Dijkstra but had years of experience making reasonably complex real-time systems work reasonably well.

Their arguments usually boiled down to the following: When a program is constructed as a single main polling loop and all action routines are called from within this loop, it is easy to assure that the program meets real-time constraints. Each routine called from within the main loop can be given a strict time limit, and it is fairly simple to show that each routine lives

within this limit.

Within action routines called from the main polling loop, some fairly simple rules must, of course, be obeyed. Straight-line code is easy to verify, branching code is easy to verify, and definite loops can be verified, but indefinite loops are forbidden.

If you look at typical real-time programs of the 60's and 70's, these rules weren't much trouble. User interfaces were crude at best, and most of the processing was fairly simple feedback control with little algorithmic complexity. Unfortunately, many of the larger problems we face today are far more complex, with significant algorithmic components.

The very coding constraints that allow straightforward verification that a program meets simple real-time constraints serve to obscure the algorithmic structure of the program. When one or more logical tasks within a real-time program involve complex algorithmic structures, they must usually be recoded using state machines that make a state transition each time they are called from the main polling loop.

As a result, it remains easy to verify that the complex tasks do not consume more than their allotted time slots in the main polling cycle, but that is all. All other aspects of the complex tasks are hidden in a mass of state machines so that even simple questions can take hours to answer. In fact, this structure can even impede the verification that some real-time constraints are met. Consider the problem of verifying the real time behavior of a logical task that, after detecting an event, must respond after a computation that requires multiple iterations of the main loop.

Douglas Jones, University of Iowa, jones@herky.cs.uiowa.edu

---

## **✂ Single Point of Failure for Internet Management**

*Kee Hinckley <nazgul@apollo.com>*

*Fri, 21 Jul 89 10:53:53 EDT*

The Boston Globe today (Fri, July 21) reported that the GAA has recommended that an advisory committee be set up to run the Internet since there was "no one as the wheel" in the latest virus incident. It seems to me that this potentially slows down the response time of the Internet to such problems and creates a single point of failure (cut out communication to the committee and now no one knows what to do).

-kee

---

## **✂ DARPA contract & AI for moving targets**

*"FIDLER::ESTELL" <estell%fidler.decnet@nwc.navy.mil>*

*20 Jul 89 08:19:00 PDT*

Two points:

1. Many years ago, the single integrated target list was for a war, that included by implication nuclear war. But even in nuclear war, NOT EVERY weapon used will be nuclear. There are some missions where conventional albeit "smart" weapons would really be better. It follows that we - and they - really do need to target things that move; e.g., large ships, and mobile missile launchers.

2. A large ship is almost equivalent in population and technical complexity to a small town; e.g., 5000 "residents" with enough "restaurants" and "movie theaters" to serve them. Recent news item: The USSR is developing for deployment its first aircraft carrier.

The technical points of "how to select" targets are a fertile question for RISKS. If and when we want to debate the policy, maybe we should move that to ARMS-D@XX.LCS.MIT.EDU

Bob

---

## ✂ Two-Word Last Names and Other Amusing Database Stories

<MCCELLELAND\_G@CUBLDR.Colorado.EDU>

Thu, 20 Jul 89 09:51 MST

Two amusing computer-related security stories from the Univ. of Colorado:

1. Bank Card Numbers for Everyone: Continuing Education offers community courses and unlike other units of the university is therefore compelled to accept bank cards for payment. This necessity was overlooked when the new student information system was created so no protected field was allocated to hold bank card numbers and no otherwise unused field appeared to be big enough. But someone cleverly decided to use an unused address field for this purpose until it was discovered that almost anyone with any access to the system could then read a student's name, address, and VISA number.

2. Another Two-Word Last Name Problem: The Colorado Association of Research Libraries now offers an on-line database of citations for every article in every journal any of the libraries receive. It isn't as good as services offered by DIALOG or ISI or other big commercial operations but it is a boon to local researchers. They offer it free to university folks but want to sell the service to outside users. Hence, all faculty now need user ids. They cleverly use SSN and last name and both are displayed when you type them on a public terminal. But mine wouldn't work! I called the CARL office and once I identified myself as a confused faculty member the cheerful clerk gladly told me my proper user id over the phone. [I thought about asking her how she knew I was who I said I was but the risks seem to be all theirs and not mine so I didn't bother.] It turns out one must add the prefix "A9/" to the SSN [maybe they added that for security :-)]. But mine still wouldn't work. Then she discovered that on the university payroll tape that had been used to create the user database my name had been entered as "Mc Clelland" so that forevermore my CARL name would be "Mc". That worked fine.

Gary Mc [Clelland]  
mcclella@colorado  
gmcclella@clipr.colorado.edu

---

**✂ Credit card issuers invade cardholders' privacy**

Andrew Klossner <andrew@frip.wv.tek.com>

Thu, 29 Jun 89 16:59:48 PDT

Excerpted from "The Facts About ... Credit Cards," in the April 1989 issue of "Vis a Vis" magazine, "The Magazine of United Airlines, Inc.":

"Enhancement" is industry parlance for the tie-ins, upgrades, rewards, automatic insurance and warranty protection for products bought with the card. Issuers continuously sweeten the enticements ...

Shopping for clothes? Traveling abroad? Do you prefer bespoke British tailoring? Country inns -- in New England or France? Your card company will soon know a thing or two about your tastes in restaurants and may some day [sic] be a source of recommendations for lodging, dining and a host of other services.

Card companies are investing huge sums of money to read and analyze your charge receipts. The "enhancement wars" create handy perks, but the battle for the hearts and minds of cardholders also rages in computer banks across the country ...

The payoff for issuers who successfully use technology to analyze customer spending will be tremendous, asserts John Love of "Credit Card News." "This information is extremely personal to the customer," he says. "He might begin to feel that his card company really understands him."

Chenault of American Express says his company is "betting the ranch" on its \$100 million Genesis Project. The program's goal is to make sure the company's nearly 300 mainframes and minicomputers can create dossiers on the tastes of cardholders. Says Chenault: "If a cardmembers is traveling to Paris, we could develop a personalized itinerary before he even gets there. We'll know his tastes in restaurants, special interests and shopping, and we could work with establishments to arrange even big-ticket purchases."

Sigh.

-- Andrew Klossner (uunet!tektronix!frip.WV.TEK!andrew) [UUCP]  
(andrew%frip.wv.tek.com@relay.cs.net) [ARPA]

---

**✂ Re: windowless cockpits**

Andrew Klossner <andrew@frip.wv.tek.com>

Fri, 30 Jun 89 09:39:04 PDT

"Video and graphics processing is performed, and digitized pictures are relayed to the helmet display."

It's the graphics processing that offers the most promise. Some projects (sorry, I have no references) are investigating the effect on military pilot performance when the visual display is \*simplified\*, to the point where important objects in the field of view are reduced to wireframe figures, and unimportant objects are eliminated altogether. Thus, an approaching mountain might look like an inverted cone sticking up ahead of you; a river underneath (or civilians about to be bombed) wouldn't be visible at all; and aircraft around you would show as stick figures, perhaps with color coding to convey relative velocity, friend-or-foe evaluation, etc. An approaching missile might look like a line growing toward you, just like it does in the "missile attack" video games.

The win is that humans are better at pattern recognition when the patterns are simple and the distractions are eliminated, especially in time-critical situations. Look at how well we do at those video games.

Another win is that, since the pilot no longer needs visual input besides the (relatively low-bandwidth) wireframe presentation, it becomes that much easier to move the pilot outside the plane, perhaps to a bunker on the ground, and run the plane by remote control. The only important sensory input that would be missing is acceleration (including gravity, "which way is down"), and good pilots learn to distrust that anyway.

But there are still occasions when you need a full-video picture, such as evaluating damage to an enemy aircraft (is it on fire?) or locating an emergency landing site. And simplified video presents new opportunities for defensive counter-measures -- you'd like the enemy's system to classify your fighter as "unimportant," or to classify your chass as "important."

"... the possibility of crashing an airplane because of a failure in the video system, coupled with the inability to look out the window (because the plane doesn't have one) is terrifying."

This risk should be kept in perspective. For example, on a high performance aircraft with forward-swept wings, if the computer handling flight stability goes down, it doesn't much matter whether the pilot can see or not; the plane is going to crash.

-- Andrew Klossner (uunet!tektronix!frip.WV.TEK!andrew) [UUCP]  
(andrew%frip.wv.tek.com@relay.cs.net) [ARPA]



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 9: Issue 9

Monday 14 August 1989

## Contents

- [California to escrow electronic vote counting software](#)  
[Rodney Hoffman](#)
- [Voters Left off Electoral Roll](#)  
[Rohan Allan Baxter](#)
- [Beeperless remote answering machine risks](#)  
[Peter Scott](#)
- [Computerized Houses](#)  
[Jake Livni](#)
- [Automated Driving](#)  
[Ian Gent](#)
- [Marijuana Virus wreaks havoc in Australian Defence Department](#)  
[J. Holley](#)
- [Universal Trapdoors](#)  
[Vin McLellan](#)
- [Computer Problems at Saratoga Racetrack](#)  
[Rodney Hoffman](#)  
[Dave Fiske](#)
- [RISKS summer reruns?](#)  
[Daniel F. Fisher](#)  
[Jim Horning](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **California to escrow electronic vote counting software**

*Rodney Hoffman* <[Hoffman.ElSegundo@Xerox.com](mailto:Hoffman.ElSegundo@Xerox.com)>

14 Aug 89 08:02:12 PDT (Monday)

Edited excerpts from an article by William Trombley in the 'Los Angeles Times' 14-Aug-89:

A new law which takes effect Jan. 1, 1990, requires California counties to place the source code of their vote-counting computer programs in escrow so they can be checked by independent experts in case of disputed results. The law is a partial response to increasing criticism that electronic vote

tabulation sometimes is inaccurate and is vulnerable to tampering because of lax security.

The California secretary of state will approve escrow facilities and will determine what material should be placed in escrow and under what circumstances the source codes should be made accessible to investigators. The escrow plan also allows election officials access to the codes should the companies that produce the software go out of business or stop selling that particular product, as has happened in several states.

California's new law coincides with efforts by the National Clearinghouse for Election Administration, an arm of the Federal Election Commission, to produce voluntary state standards for computerized elections. The federal standards, published in the Federal Register last week, also call for putting source codes in escrow. So far, Texas, New York and a few other states have laws similar to California's.

Reactions to the new law vary:

Tom Diebold, president of DFM Associates, one election system vendor: "The problem with escrow is that it makes it easier for someone who wants to manipulate an election to get their hands on the source code."

Lester Jaspovice, V.P. and corporate counsel for Sequoia Pacific Systems, another vendor: "My company doesn't like it, but, as an attorney, I think it's a good idea. It provides a virgin copy of the code that the court can call on in case of a dispute."

Howard Strauss, Princeton University computer scientist and member of Election Watch: If the source code in escrow differs from the one used to count votes, "then you know something's wrong. But if they're the same, it doesn't tell you anything because they could both contain the same mistakes." Strauss also doubted that the law would protect against a company going out of business or losing its top scientific talent. "The idea is that these escrow facilities will have technical people who can read this stuff, but some of it is so badly written that, even after months of work, you wouldn't know what it was all about."

Crew Deer, V.P. of Data Securities International, a computer software escrow company: "If the code has a bug in it, it will show up on both the original and the copy, but that's good because you at least know it's a technical problem and nobody has been tampering." According to Deer, the escrow fees for vote-counting source code might be about \$1500 plus \$1000/year after that. If a result is challenged and a detailed verification process is carried out, the cost could be as much as \$30,000.

Several critics said the new law does nothing to correct what they consider to be the major flaw in computerized elections -- the presence of poorly trained, underpaid election workers who do not understand the computerized equipment they are using to count votes.

[For the record, on July 2, 3, and 4, the 'Los Angeles Times' ran a very lengthy series by William Trombley on computers and vote counting. Nothing new, but a fair summary of past troubles, present systems, and suggested

changes.

It includes quotes from many election officials, computer scientists, and statisticians. Among those cited are RISKS contributors Gary Chapman and Marc Rotenberg of Computer Professionals for Social Responsibility, Lance Hoffman of George Washington University, Willis Ware of RAND, and RISKS moderator Peter Neumann. (See [RISKS 7.52](#) and 7.70 for references to past reports on the subject.)]

---

### **✂ Voters Left off Electoral Roll**

*Rohan Allan Baxter <rohan@bruce.cs.monash.OZ.AU>*

*Thu, 10 Aug 89 08:21:34 EST*

More than 6000 voters were unable to vote in local government elections in Victoria on Saturday, August 5th, because of a computer error made by the Australian Electoral Commission. Newly enrolled voters and those who had changed municipalities had their names left of the updated electoral rolls.

The error was made five months ago, but was detected less than 24 hours before the opening of the polling booths. A full internal inquiry has been ordered into why the error was detected so late, as well as its original cause.

Legal opinion indicate the elections are not invalidated by the error, although legal challenges are expected from narrowly losing candidates. One bitter voter affected by the error noted that voting in the elections was compulsory - a bitter irony for those left of the rolls.

---

### **✂ Beeperless remote answering machine risks**

*Peter Scott <PJS@grouch.JPL.NASA.GOV>*

*Sat, 5 Aug 89 14:28:03 PST*

My answering machine is one that allows me to call in from a push-button phone and signal it to play back my messages with a 2-digit code. In addition, there are single-digit codes that reset the machine, go forwards, backwards, change the outgoing message, etc.

I just called in to get my messages; there was one. Just before the caller hung up they accidentally bumped some keys on their phone, resulting in some digit tones being recorded on their message. I heard this and waited for the machine to beep to tell me it had finished playback. Instead, it played the message again... and again... Apparently it was taking input from the message tape as valid, and one of the buttons the caller pressed was the "backwards" command.

I suppose if I were getting the message off the machine at home this wouldn't happen, because it would not be in remote mode. This has some interesting consequences for the unscrupulous callers and unwary callees.

Peter Scott (pjs@grouch.jpl.nasa.gov)

---

## ✂ Computerized Houses

Jake Livni <JAKE%Irving@VX1.GBA.NYU.EDU>

Mon 14 Aug 89 18:57:48-EDT

"The New Homes Are Getting Smarter"

"Cued by computers, they run themselves"

by Mark McCain

(Excerpted from the Real Estate Section of the New York Times, August 13, 1989)

Although electronic brains these days control televisions and telephones, offices and automobiles, the average house is still a mindless creature, bumbling along without any effort to make itself more safe [!!!], or economical, comfortable or convenient.

For many homeowners, that's fine. The thought of a house smart enough to take matters into its own hands is absurd - even threatening. Who's to say it wouldn't fire up the oven after midnight just on a lark?

But new houses are improving their IQs. After many years of futuristic talk without much follow-through, builders are beginning to install automated systems that act like all-knowing butlers. Not surprisingly, the systems are most popular in expensive houses, where budgets are big and rooms so numerous that even turning off lights at bedtime can be burdensome. [...]

"When my 3-year-old boy comes out of his room at night, a motion detector turns on the hallway light for him," says Robert Pomeranz, a banking executive who lives in a new 7,500-square-foot house outside Washington. "Obviously, it's not worth buying an integrated control system for small things like that, but it's amazing how useful the system can be as you become comfortable with it."

Like humans, the systems aren't perfect. A light may turn on for no apparent reason or a front door may refuse to open for it's master.

[That sounds nice in an emergency...]

"The houses we're building today have interiors right out of the space age, even though their exterior appearances are traditional," said Kenneth Nadler, an architect in Mount Kisco, NY, who designs expensive houses. "It's Jetson on the inside and Gatsby on the outside."

For a homeowner eager to outdo even George Jetson, the futuristic TV cartoon character, there's a \$26,000 whirlpool that accepts calls - say, from a car phone - to start water running at bath-perfect temperature. Too expensive? For less than \$1,500, there's a fireplace with a gas flame adjustable from glowing to roaring by infrared remote control.

[Could Audi 5000's order up a bath by themselves? :-) ]

But even aficionados have their limits.

"I'm afraid of those things," said Joel Sommer, a Maryland builder who infuses his multi-million-dollar houses with high technology. "What would happen if the whirlpool didn't shut off automatically or gas started flowing in the fireplace without an ignition spark? I just don't see the benefit of some products."

Certainly, automated devices built into houses today do not always make practical sense. It is a situation reminiscent of the home-computer craze in the early 1980's, when companies promoted computers for such uses as storing recipes, even though ingredients that only soil a cookbook page might easily destroy a kitchen keyboard. Today home computers are common, but not for recipes or checkbook balancing or other uses suggested by early promoters.

"In similar fashion, I'm sure we'll find a great many applications for home automation that people haven't thought of yet or haven't predicted to be big winners," said Roger Dooley, editor of *Electronic Home*, a trade magazine published in Mishawka, Ind. "And what's being touted today as big benefits may end up being used by only a few homeowners." [...]

"I live alone in a 10,000-square-foot house with only my housekeeper, so I need to feel really secure, and what I've installed is state-of-the-art," said [... someone who has such a system. She also ...] has a sensor in each room to control the temperature, and only once have things gone awry. "During a storm with heavy lightning the sensor in the living room got stuck at 95 degrees," she said. "So the air-conditioning system kept trying to cool the room. It felt like a meat locker." [...]

Beyond that, there's the gee-whiz appeal, like a synthesized voice in the kitchen that announces when a letter carrier has delivered the mail. [...] "You don't have to install an integrated control system," said Mr. Sommer, the developer, who is completing an 11,000-square-foot house with such a system. "I happen to enjoy them because my background is in computer science. But really, they're toys."

[discussion of business aspects of marketing these systems...]

One futuristic idea now becoming more practical is voice control. Already, voice-recognition devices that allow a computer to understand a vocabulary of about 75 words are available for less than \$500. As those devices become more powerful and less expensive, they will be an option for controlling home automation.

"You'll be able to just walk up and talk to it," explained David MacFadyen, an industry expert. "When you say, 'Good night, house,' the temperature controls will be set back in unoccupied areas, the hot-water heater will be set back, the phone will go on voice-mail. Just a couple of words will trigger an evening shutdown sequence that is far more elaborate than anything we can think of now.

["Good night, RISKS" ...

--> EXIT, SEND, QUIT, LOGOUT]

Jake Livni

---

## ✂ Automated Driving

*Ian Gent <ipg@cs.warwick.ac.uk>*

*Mon, 14 Aug 89 14:48:31 +0100*

A documentary on UK's Channel 4, 13 Aug 1989, was about traffic problems, especially congestion in cities.

After concluding that there was no obvious and fair solution, the programme suggested that the best hope lay in more automation in cars. What's more, the programme implied that machines driving cars would be feasible in the medium term (next decade or two).

For instance, shots were shown of a human driven automobile in which experimenters were recording data about close vehicles, etc. Apparently, and I paraphrase the commentator, although the researchers were only recording data, there's no reason in principle why the information should not be fed into control computers. The clear implication was that this would be much safer than letting humans drive.

Also, with automatically or semi-automatically driven, it would be possible for my vehicle to refuse to let me drive into a city centre if the centre was too busy.

The risks are obvious and horrific, but what is even more depressing is that experts in other fields just do not see the risks, and that TV researchers do not even think to ask anybody who might know about these risks.

Ian Gent, University of Warwick, Coventry, UK

---

## ✂ Marijuana Virus wreaks havoc in Australian Defence Department

*<J.Holley@MASSEY.AC.NZ>*

*Mon, 14 Aug 89 10:18:16 NZS*

Quoted from The Dominion, Monday August 14 :

A computer virus call marijuana has wreaked havoc in the Australian Defence Department and New Zealand is getting the blame.

Data in a sensitive security area in Canberra was destroyed and when officers tried to use their terminals a message appeared : "Your PC is stoned - Legalise marijuana".

Viruses are [guff on viruses] The New Zealand spawned marijunana has

managed to spread itself widely throughout the region.

Its presence in Australia has been known for the past two months. The problem was highlighted two weeks ago when a Melbourne man was charged with computer trespass and attempted criminal damage for allegedly loading it into a computer at the Swinbourne Institute of Technology.

The virus invaded the Defence Department earlier this month - hitting a security division responsible for the prevention of computer viruses.

A director in the information systems division, Geoff Walker said an investigation was under way and the infection was possibly an embarrassing accident arising from virus prevention activities.

New personal computers installed in the section gobbled data from their hard disk, then disabled them.

Initially it was believed the virus was introduced by a subcontractor installing the new computer system but that possibility has been ruled out.

One more outlandish theory suggested New Zealand, piqued at its exclusion from Kangaroo 89 military exercises under way in northern Australia, was showing its ability to infiltrate the Canberra citadel.

New Zealand was not invited to take part in Kangaroo because of United States' policy of not taking part in exercises with New Zealand forces since Labour's antinuclear legislation. However, New Zealand observers were invited.

New Zealand Defence Department spokesmand Lieutenant Colonel Peter Fry categorically denied the claim. "It would be totally irresponsible to do this kind of thing."

In fact, New Zealand's Defence Department already had problems with the virus, he said.

---

## **✂ Universal Trapdoors**

*<McLellan.Catwalk@DOCKMASTER.NCSC.MIL>*

*Sat, 5 Aug 89 22:06 EDT*

If most large-system sites have user-installed trapdoors...

If techies and technical management install these trapdoors to evade the access control tables because they are convinced these subsystems are 1) too often mismanaged, 2) too easily corrupted, 3) too cumbersome in an emergency, or 4) too prone to technical failure...

Then -- so long as this huge community of unbelievers remains unwilling to submit to the control of the access control system -- we will have users installing trapdoors for an alternative path to

high-privileged status, despite the obvious risks.

If 15 years of unrelenting propaganda by the vendors and gurus have left the users so unwilling to follow the prescribed path of righteousness, maybe someone other than the users should reconsider. As it is, user-installed trapdoors are almost universal on big systems, but because they are illicit, "secret," they are seldom protected by anything more than their obscurity.

What is so wrong about giving the users a safe model for what they demand -- a route around the access control system -- when just they take it anyway, security be damned?

Who is being more unrealistic: the system programmers who code these traps, or the security specialists who ignore the fact that virtually all systems have trapdoors? Aren't we talking about trusting people who are already virtually all-powerful in their environment?

Why can't we use an alternative security device to secure this alternative access path? Encryption seems a likely padlock. With a mix of synch and asynch crypto, it seems possible to set up a "one-time key" access, supported by user authentication, separation of function, audit trails. Heck, add an audible alarm. Even without the PKE frills, simple encryption can put a lock on what is otherwise an open gate hidden in the thickets. Continuing the masquerade, ignoring the existence of the problem, gets us Nowhere.

For twenty years people have been showing me trapdoors into systems. Now, I'm shown or told of trapdoors that open whole networks (recently, one which popped a net of control systems for a major phone company, installed by management.) Now, I chat with hackers who give tutorials on how to locate user-installed trapdoors. One "specialist" recently told me that it seldom takes him more than 20 minutes to identify such a trapdoor in a typical corporate MVS system.

The auditors are not the only ones, nor likely the most challenging foe, these users have to outsmart.

Vin McLellan The Privacy Guild (voice/fax: 617-426-2487) Boston, Ma. 02111

---

## **✂ Computer Problems at Saratoga Racetrack**

*Rodney Hoffman <Hoffman.ElSegundo@Xerox.com>  
4 Aug 89 07:23:56 PDT (Friday)*

From wire service stories in the 'Los Angeles Times' August 3 and 4, 1989:

Computer problems frustrated a record opening-day crowd at New York's Saratoga Race Track on Wednesday, and track officials said Thursday's card might be canceled if the problem was not fixed by Thursday morning. Bettors were kept in the dark about the odds, payoffs, and even the time of day.

"There's some sort of gremlin running around that software, and we can't find it," said Gerard McKeon, president of the New York Racing Assn on Wednesday. ... The computer problem extended Wednesday's nine-race card by an hour and cost NYRA about \$1.5 million in handle, McKeon said. Pari-mutuel machines and the track's tote boards were also affected by the problem.

Technicians worked through the night to replace the software, and things were apparently back to normal on Thursday.

---

### **✂ Computer Breakdown Thwarts Saratoga Bettors**

*Dave Fiske <davef@brs pyr1.brs.com>*

*3 Aug 89 21:35:32 GMT*

Here's a first-hand account of an item for RISKS, since I was there on Wednesday.

August 3, 1989, Latham, NY

Yesterday was opening day for thoroughbred racing at the Saratoga Race Course in Saratoga Springs, New York.

It was a computer disaster.

The beginning of the 122nd season was ruined by computer problems which forestalled the placement of wagers for Races 5 through 9 of the 9-race program. The New York Racing Association, which operates Saratoga and the other racing facilities in New York, is estimating a loss of \$1.5 million in on-track, and \$2 million in off-track handle. The loss in good will is not measurable--parimutuel systems are dependent on their accuracy and reliability for continued patronage--chances are most fans will be forgiving and come back. Provided, that is, that the system gets straightened out.

This is by no means certain. Racing officials announced yesterday that they had no idea what had caused the computer system to crash, and for fans to listen for a 9 AM announcement this morning before heading for the track. This morning, NYRA announced that they intend to offer wagering today, that they believe they have found the software problem and corrected it, and that they are "80%" sure the system will work correctly once betting begins today.

Like most tracks, betting information is displayed both on Tote Boards (light-bulb displays) and on computer-generated video screens. Both types of displays were affected by the problem(s)--at one point, I observed that odds displayed on the two types differed. (Presumably one was being updated from the computer, and the other not. However, regardless of which was correct, some fans were being provided with inaccurate information.)

Though the displays worked on and off from the 5th race on, the betting machines did not function at all. The machines are of two

types--terminals which are located at the regular betting windows, and which are operated by track employees; and so-called "SAMs", which employ touchie-feelie screens so that bettors can place their own wagers. The self-service machines allow a bettor to insert a winning ticket or a cash voucher. Under ordinary circumstances, the value of the ticket or voucher is read and then displayed on the screen. At the beginning of the computer outage, machines were displaying incorrect values for tickets, or simply eating tickets or vouchers. Bettors who had encountered problems at the betting windows at least had a human clerk to complain to--those using the SAMs had to stand around wondering what to do.

Post times for races were delayed in hopes that the computers could be made to operate, but to no avail. The final race took place nearly an hour later than usual--and only those few who had made advance wagers early in the day had any money riding.

Because the system handles both bets and payoffs, automated calculation of prices for winning horses was also pretty much incapacitated. People holding winning tickets (even from previous races) were not able to cash them.

Technicians worked overnight, having flown up from Autotote in Delaware, and apparently fixed some software problems, but officials still are not certain of what happened exactly.

Today, Thursday, the system seemed to operate properly. The normal \$2 admission fee was waived, as a gesture to yesterday's disappointed fans. However, given that officials were uncertain this morning that it would hold up, the system's performance may have been more luck than anything else.

Other than having diagnosed the problem as a software, rather than a hardware, one, officials are offering no explanation as to what the problem was. However, as an outsider, one could focus on the following factors:

When the season at Saratoga starts each year, most of the equipment used is moved up from Belmont Park, near New York City. The move, which includes starting gates, etc., as well as the computers, betting machines, and TV monitors, takes place in the timespan from the last race at Belmont on Monday to the first race at Saratoga on Wednesday. Assuming that no hardware damage occurred in transit, this allows very little time for testing, since some of those 30-40 hours are taken up by travel time and installation.

Though officials say that software changes are made nearly every week, a number of changes--some in effect only for the Saratoga meet--were made in the betting rules. For example, Triple betting is now offered in the 8th as well as the 9th race; the number of horses required to be entered in races offering certain exotic wagers was lowered; and for two racing days only, when important stakes races are run, exacta wagering will be allowed for all races, regardless of the number of horses entered.

My guess is that more--and more sophisticated--software changes were made than

normally, and that, with limited time to test a system which was asked to handle wagers from 30,000 people yesterday, some bug went undetected until triggered yesterday.

It will be interesting to find out what backup setup NYRA utilizes. Officials mentioned today that, if the system broke down today, that hopefully their backup systems would not fail, so that they could determine what went wrong. This leads me to believe that there was a secondary failure of some type yesterday, such that the planned backup process did not work.

---

### **✂ RISK summer reruns?**

*Daniel F. Fisher <dff@Morgan.COM>  
Fri, 4 Aug 89 22:32:43 EDT*

During the present slow-down in RISKS, I was particularly happy when, this evening, my netnews reader presented me with an `unread' RISKS digest. It was not until I was half way through it that I realized it was one I had already seen. In fact it was [RISKS 8.81](#) from 17 June 1989. Was this a local phenomenon, or has the Network, not wishing to RISK lower ratings, started airing Summer Reruns?

Just curious,

Daniel F. Fisher, Morgan Stanley & Co. Inc.

---

### **✂ For your amusement [ RISK summer reruns? ]**

*Jim Horning <horning@src.dec.com>  
2 Aug 1989 1828-PDT (Wednesday)*

Here's the Path: on the copy of [RISKS 8.81](#) that just arrived!

Path: jumbo!decwrl!purdue!mailrus!csd4.milw.wisc.edu!leah!rpi!batcomputer  
!cornell!rochester!rit!tropix!moscom!ur-valhalla!uhura.cc.rochester.edu  
!sunybc!rutgers!cs.utexas.edu!tut.cis.ohio-state.edu!ucbvax!KL.SRI.COM!RISKS



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 9: Issue 10

Monday 14 August 1989

## Contents

- [KAL007 - jury finds "willful misconduct"](#)  
[Clifford Johnson](#)
- [California studies "drive-by-wire"](#)  
[Rodney Hoffman](#)
- [NY State DMV Computer RISKS](#)  
[Will Martin](#)
- [RISKS is back in gear \(almost\)](#)  
[PGN](#)
- ["Radiation" or "Fields"](#)  
[Jerry Leichter](#)  
[Irving Wolfe](#)  
[John H. Martin](#)  
[Irving L. Chidsey](#)  
[Klaus Rieckhoff](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✉ KAL007 - jury finds "willful misconduct"

"Clifford Johnson" <[GA.CJJ@Forsythe.Stanford.EDU](mailto:GA.CJJ@Forsythe.Stanford.EDU)>

Thu, 3 Aug 89 08:59:49 PDT

New York Times, Aug. 3 (Richard Witkin):

Families of victims of the 1983 downing of a Korean Air Lines jumbo jet by a Soviet fighter may collect unlimited compensatory damages from the airline because of the crew's "willful misconduct" in straying over Soviet air-space, a Federal court jury in Washington ruled yesterday . . . The term is legally defined as an intentional act performed with knowledge of likely injury to passengers or "with reckless disregard of the consequences." . . . Judge Robinson earlier dismissed lawsuits against the Soviet Government; the Boeing Company, the builder of the 747; Litton Industries, which made its navigation systems; and the United States

Government, which employed the traffic controllers involved in the first part of the flight.

N.B. The suit against the U.S. government was dismissed at the outset of the case some years ago, on the "ground" that the court refused to countenance U.S. government involvement; and a gag order was placed on government employees.

---

## **California studies "drive-by-wire"**

*Rodney Hoffman <Hoffman.ElSegundo@Xerox.com>*

*2 Aug 89 17:50:17 PDT (Wednesday)*

Summary of a lengthy article by William Trombley in the 'Los Angeles Times' 24-July-89:

The California Dept. of Transportation (Caltrans) has begun its most ambitious research program, ranging all the way to "'Star Trek' systems that would propel 'platoons' of vehicles down automated freeways at 70 mph with only 50-foot separations between cars."

"In some areas, like Los Angeles, there's no more room for new freeways and the next advance has to be technological," says Caltrans Director Robert Best. "We've paved the world, especially in the Los Angeles area," says UC Davis mechanical engineering Prof. Andrew Frank, "and now we've got to make much more use of that pavement."

Caltrans' new Office of Traffic Improvement has spent about \$6 million so far, with most of the money going to the Univ. of California's Institute of Transportation Studies, which is sponsoring research by at least two dozen faculty members on several campuses. Most of the work has been gathered together in the Program on Advanced Technology on the Highway (PATH), which includes research on navigation, electrification, and automated highways.

The article reviews a number of real and imagined systems. One real one is Pathfinder, a straightforward CD-based navigation system soon to be tested in 25 test cars for use along LA's Santa Monica Freeway. Other projects study electric vehicles, human factors ("how effectively drivers use automated equipment") and road pricing -- charging motorists to use automated highways, including higher rates at peak hours.

One complex project studies radar-equipped and computer-controlled cars, held in the center of the lane by a lateral guidance system that depends on electric sensors placed in the roadbed and provided with "a smarter version of 'cruise control'" called longitudinal control -- moving cars at high speed without crashing into one another. The radar system is to be tested later this year with a "platoon" of six cars along an interstate highway north of San Diego (in a reversible lane unused during mid-day). The radar collision-avoidance system costs about \$10,000 per unit now.

A few key quotes from the final sections of the article:

A major question is this: How will the public react to a system that

takes decisions out of the hands of the individual driver and gives them to a computer?...

A second problem is what to do with all the new vehicles that a more efficient road system would accommodate. Where will they park?...

Then there is the question of liability... the Achilles heel of this research effort. "This system would be much safer than what's out there now," says PATH Director Robert Parsons, "but with this technology, you can trace fault [for accidents]. How do you limit liability and keep the 'deep pockets' thing from killing us before we get started?"

---

### **✂ NY State DMV Computer RISKS**

*Will Martin <wmartin@STL-06SIMA.ARMY.MIL>  
Tue, 1 Aug 89 10:19:35 CDT*

The following brief item was in the "Regional News" section of the July 31, 1989, issue of CITY & STATE, a slick-paper tabloid trade paper for local government topics, page 22:

#### COMPUTER SECURITY FAULTED

A dearth of safeguards for the state computers that hold information on New York's drivers could allow system users to erase driving convictions and wipe out other records, state Comptroller Edward V. Regan has charged. The state Department of Motor Vehicles also lacks contingency plans to keep its computers running if a disaster shuts down operations at the agency's computing center, Mr. Regan said. He recently made the charges in an audit that reviewed security and disaster planning at the center between April 1987 and March 1988.

That's all the info I have; maybe some NY-state people have more info from their local media on this topic.

Will Martin

---

### **✂ RISKS is back in gear (almost)**

*Peter G. Neumann <Neumann@KL.SRI.COM>  
Mon, 14 Aug 89 20:00:01 PDT*

After a few exciting moments with airlines and some eccentric East-coast weather, I am back on the West coast, but backlogged with 17 days of EMAIL. Flying is not what it used to be. But then, as Arthur Clarke once lamented, regarding how difficult writing good science fiction was becoming, "The future isn't what it used to be." On the other hand, judging from the material waiting for [RISKS-9.9](#), there are still lots of topics ready for this forum, and RISKS is again in there ready to dig it out for you.

However, I see that I am not quite fully in the swing of things. Before

everyone jumps on me, let me apologize for not setting the date on the masthead of [RISKS-9.9](#), which of course should have been \* 14 Aug 1989 \*. With some people having gotten a net-gratuitous copy of [RISKS-8.81](#) a month and a half late, I needn't have added further to the confusion. Sorry!

By the way, I hope to move RISKS from KL.SRI.COM to CSL.SRI.COM this month. The archives will probably move to CRVAX.SRI.COM, because the KL is being decommissioned. The mailing list differences should be sorted out very soon, but a few of you may experience some bumps in the process. There are also a bunch of nonworking addresses at the moment, and I am hoping that the CSL (Sun) mailer tables will simplify matters. (For example, the KL does not let me ANSWER mail from BITNET or UUCP, while the CSL does. That is a real pain.) So, a little patience is in order. Thanks. Peter



<"Jerry Leichter - LEICHTER-JERRY@CS.YALE.EDU">

Thu, 20 Jul 89 12:30 EDT

<LEICHTER@Venus.YCC.Yale.Edu>

Subject: "Radiation" or "Fields"

In [RISKS 9.7](#), Jan Wolitzky takes Gordon Hester to task for distinguishing "fields" from "radiation" in discussion the hazards of ELF electromagnetic sources.

It is quite true that "radiation" is the scientifically correct word across the entire electromagnetic spectrum. But things are not quite that simple. When we think about an electromagnetic radiator, we almost always think of its "far field" - the region in which it behaves in the familiar way as a traveling wave of crossed E and B fields. But there is also a "near field" region with quite different characteristics. It's been way too many years since I looked at this stuff, so I can't vouch for any of the details, but as I recall near field effects drop off exponentially, so are not an issue except very close to the radiator. But near enough, they are dominant.

If you think only in terms of far field effects, you are hard pressed to explain how a transformer can possibly work at 60 Hz - the "radiator" and receiver are tiny fractions of a wavelength long!

When one talks about shielding for appliances, one talks about shielding the magnetic and electric fields independently. This would be meaningless in the far field, where the connection between the two is fixed.

I'm not certain that it was this distinction that Hester was getting at, nor do I know exactly what the significance of the near/far field distinction in this area is - though I expect its essential: The far field produced by any object the size of an appliance at 60 Hz must be minuscule. (Note that this may be very different from a power transmission line.)

-- Jerry

## ✂ New Yorker Radiation Articles by Paul Brodeur

Irving Wolfe <irv@happym.wa.com>

21 Jul 89 18:52:15 PDT (Fri)

Unlike Gordon Hester in volume 9, issue 6, I found Paul Brodeur's series of three articles in The New Yorker Magazine balanced and fascinating. He discusses the clearly-shown (epidemiologically & statistically, not by argument based on theoretical considerations) health effects of three different types of non-ionizing radiation. At least one of these -- magnetic fields from CRT terminals -- most readers of Risks are probably heavily exposed to.

These articles seem so worth reading that I will refrain from providing any summary at all. The New Yorker is available in most good libraries, and the stories appeared in successive issues beginning June 12.

Rather than be dissuaded from reading them by Mr. Hester's comments, go to the library and judge for yourself.

---

## ✂ Radiation (Re: [RISKS-9.7](#))

<ksr!johnm@harvard.harvard.edu>

Fri, 21 Jul 89 20:00:18 EDT

I have some real problems with Jan Wolitzky's comments on Gordon Hester's review of Paul Brodeur's New Yorker article.

Wolitzky's high school education seems to have been an example of the crisis in science education we hear so much about. The correct technical term is field. (I have a Ph.D. in chemical physics, and in a former life taught some of the introductory physics courses at Harvard, so I think I'm on reasonably safe ground here.)

The purest example of the difference between the electromagnetic field and electromagnetic radiation is a static charge - a charged capacitor doesn't radiate at all but it certainly has an electric field. Maxwell's equations are FIELD equations that turn out to have electromagnetic radiation as one set of solutions. The quantum picture, with wave/particle duality and all that, muddies the picture a little, but in quantum physics one usually says "radiation" with the single-isolated-particle view (i.e., with single photons, neutrons, alpha particles, etc.) and "fields" with the collective-action view. In fact most of the concerns about EMF concern the near-field effects surrounding powerlines, electric blankets, computer terminals, and so on, and not the radiation from such devices, which is relatively small.

As an example of how the term "radiation" can "mislead the unwary," consider the phrase marked with carets above. In addition to its fuzziness (wavelength is inversely proportional to frequency, which is directly proportional to energy PER PHOTON; they are intimately interrelated in modern physical theory but not "different ways of expressing the same

thing"), it entirely misses the point of the difference between low-frequency EMF and ionizing radiation:

Biological effects of low-frequency EMF can't have any relation at all to individual photons -- a 60 Hz photon has a trillionth of the thermal energy surging around in a molecule at body temperature or in one of the infrared photons that swarm around us as thermal background. The normal fluctuations in a molecule's heat energy from picosecond to picosecond far exceed the energy of such a photon. Biological effects can only stem from the collective action of the field and the energy (or better, the strength) of the field, which is unrelated to its frequency and wavelength; the effects themselves may have a frequency dependence through dispersive phenomena in the body, and might also depend on the orientation of the field.

Perhaps Wolitzky needs to go back to school. Now somewhere I have a copy of Jackson's Classical Electrodynamics, crammed into my head by Nico Bloembergen (who later won a Nobel Prize for his work on lasers), that I might be willing to part with...

John H. Martin, Kendall Square Research Corporation,  
170 Tracer Lane, Waltham, MA 02154

---

**✶ Radiation ( Re: [RISKS-9.7](#) )**

<chidsey@BRL.MIL>

Thu, 20 Jul 89 11:55:22 EDT

The difference between radiation and fields is somewhat pedantic. But, if your close enough to a power line to have to worry, you are well inside the near field and the couplings wwill be much easier to compute by field theory than by radiation theory.

The differentiation from ionizing radiation is not pedantic. We have some knowledge about the damage mechanism of ionizing radiation. We have no knowledge about the damage mechanism of ELF fields except that they are subtle and almost certainly different from those of ionizing radiation.

To ignore the possibility of damage is foolish, to confuse the two is to cause confusion and unnecessary fear. We have to keep the problems separate.

Irv

I do not have signature authority. I am not authorized to sign anything. I am not authorized to commit the BRL, the DOA, the DOD, or the US Government to anything, not even by implication. Irving L. Chidsey

---

**✶ EM radiation effects**

<Klaus\_Rieckhoff@cc.sfu.ca>

Thu, 3 Aug 89 14:31:08 PDT

In 1963 (yes, I am that old), while doing nonlinear optical work at the IBM research lab. in San Jose, I was invited by people at the US-Army Medical Research Headquarters in Fort Knox, Kentucky, to give them the benefit of my advice regarding some peculiar experimental results that they had obtained and which some people there believed to be related to multiphoton absorption (on which I with some others had just published some papers).

I accepted the invitation and spent a very interesting day with them. They were a group of medical doctors and some biophysicists looking into biological EMF effects in a variety of ways. This is not the place for a general comment though I shall point out that I (a Canadian and thus a foreign national) was never asked to keep anything I saw or talked with them about confidential and, in fact, expected to see some of their work published in due course.

The specific experiment I was consulted on, looked at the the deactivation of the enzyme alpha-amylase by extremely low intensity rf fields in the region of about 10 MHz (they used an old General Radio rf generator) and the deactivation occurred (in aqueous solution, I believe) at very sharply defined frequencies that had a regular spacing with some integral relationships (I don't recall the exact details) of the spacing, something like multiples of 150 KHz and with widths of KHz.

While their results seemed to have absolutely nothing to do with my own research, as an experimental physicist I looked very carefully at their experimental setup and could find nothing wrong with it and no obvious possible explanation for their results in terms of an experimental artifact. I found the results extremely intriguing, particularly as they had found similar (although experimentally more difficult and less clear in terms of confidence) effects on gamma globulin in the region of 200 MHz.

The implications of low intensity biological effects on enzymatic activity are profound to say the least, though by their very nature they would be very difficult to pin down, particularly in complex organisms like rats or mice, let alone men (or women).

Naturally, I expected to hear more about this and over the years have broached the subject with many friends and colleagues in physics as well as biology. None had ever heard about this. Some in the 60s wrote to the people in Fort Knox about it, but never received an answer. In all the writings on the subject of biological EMF effects, for instance in reviews in SCIENCE etc., I have never heard a mention.

This is the end of the story.

Now my questions:

Has anybody heard about this type of effect? Is anybody interested in this? Has someone suggestions as to how one could (after all these years) find out more about this? I still find it hard to believe that what I saw turned out to be an experimental error of the cold fusion kind. Also, I find it still strange, that nobody should ever have tried to look for low field-strength EMF effect on enzyme activity. But then I have certainly no time to look into that kind of literature. However, some of the people I talked to should have heard about such research. None have.

Klaus Rieckhoff, Dept.of Physics, Simon Fraser University,  
Burnaby,B.C. V5A 1S6, Canada. USERKLUS@SFU.BITNET Klaus\_Rieckhoff@cc.sfu.ca



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 9: Issue 11

Tuesday 15 August 1989

## Contents

- [Cellular Telephone Causes Airliner Fire Alarm](#)  
[Dave Davis](#)
- [Computer-based airline ticket scam](#)  
[Rodney Hoffman](#)
- [1989 CPSR Annual Meeting](#)  
[Gary Chapman](#)
- [New Yorker Article on EMF Risks](#)  
[Gordon Hester](#)  
[Dan Schlitt](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✉ Cellular Telephone Causes Airliner Fire Alarm

*dave davis <davis@community-chest.mitre.org>*  
*Tue, 15 Aug 89 08:17:31 -0400*

A morning radio news report here in Washington, DC reported that a commercial airline crew noted a fire alarm signal from a cargo hold in mid-flight. Upon returning to their originating airport, the cargo hold was examined carefully, and no evidence of fire was found. Apparently, a cellular telephone in a passenger's luggage had received an incoming call, that activated the smoke (I assume) detector via RF interference.

This occurrence shows why we have systems engineers. That is, someone who must consider not only electromagnetic compatibility between system components, but also with other systems in the same operating environment. As a result of this event, the aircraft companies may have to redesign a lot of sensors.

Dave Davis, MITRE Corp., McLean, VA

---

### ✉ Computer-based airline ticket scam

*Rodney Hoffman <Hoffman.ElSegundo@Xerox.com>  
15 Aug 89 09:12:10 PDT (Tuesday)*

From the 'Los Angeles Times' 14-Aug-89:

Phoenix police arrested four people as they continued to unravel a bogus airline ticket ring that allegedly sold millions of dollars of stolen tickets by advertising discounted fares in national publications. Investigators said the individuals put together a major conspiracy by knowing how to access airline computers to put travel itineraries in the computer system.

---

### **✦ 1989 CPSR Annual Meeting**

*Gary Chapman <chapman@csl.stanford.edu>  
Mon, 14 Aug 89 13:48:33 PDT*

The 1989 Annual Meeting  
Computer Professionals for Social Responsibility  
October 20-21, 1989  
Washington, D.C.

The Friday, October 20, program of the CPSR Annual Meeting will be held in the auditorium of the Pan American Health Organization, 525 23rd Street, N.W., Washington, D.C.

Keynote speaker: Senator Patrick Leahy (D-VT), on "Technology, Privacy and Civil Liberties."

Panel discussion, "Federal Support for Computer Science R&D and the Nation's Technological Base." Moderated by Lance Hoffman, professor of computer science, George Washington University. Panelists:

Frederick Weingarten, Congressional Office of Technology Assessment  
Division of Information Technologies  
Kenneth Flamm, researcher in information technologies and public policy, the Brookings Institution  
William Scherlis, director of the software division of the Information Science and Technology Office of the Defense Advanced Research Projects Agency  
Marilyn Elrod, staff director, House Armed Services' Committee Subcommittee on Research and Development  
Ann Markusen, professor of urban planning and development, Rutgers University, nationally-known expert on the economic impact of military spending and economic conversion

Awarding of the Norbert Wiener Award for Professional and Social Responsibility to Professor Daniel McCracken of the City University of New York

Luncheon speaker: Karen Nussbaum, founder and executive director of the National Association of Working Women, or 9to5. Speaking on "Electronic Monitoring, Privacy, and Public Policy." (Faculty Club of GWU)

Panel discussion, "Computers in Education: Mixed Agendas and Uncertain Outcomes", Moderator: Terry Winograd, professor of computer science, Stanford University. Panelists:

Carol Edwards, Director of the Southern Coalition for Educational Equity and Project MICRO

Linda Roberts, Program Director, Office of Technology Assessment

Sherry Turkle, professor of sociology, MIT, author of the book, *The Second Self: Computers and the Human Spirit*

Chet Bowers, author of *The Cultural Dimensions of Educational Computing*

Panel discussion: "Patrolling the Programmers: Computer Ethics and Computer Accountability". Moderator: Rachele Hollander, Coordinator, Ethics and Values Studies Program, National Science Foundation. Panelists:

Bryan Pfaffenberger, School of Engineering and Applied Sciences, University of Virginia

John Shore, Vice-President, Entropic Systems, Inc., author of *The Sachertorte Algorithm and Other Antidotes to Computer Anxiety*

Carol Gould, professor of humanities, Stevens Institute of Technology

On Saturday, October 21, CPSR activists, leaders, and members and interested people will meet to talk about the organization. There will be workshops on computers and civil liberties, computers and the military, computers and education, and other subjects. There will be reports from the chapters around the country, and a report from the national staff about the finances of the organization.

A highlight of the Saturday program, to be held at the George Washington University, will be a workshop on local organizing led by Monica Green, National Field Director for SANE/Freeze.

For more information, call the CPSR National Office at (415) 322-3778, or write P.O.Box 717, Palo Alto, CA 94302-0717, or netmail to [Chapman@csl.stanford.edu](mailto:Chapman@csl.stanford.edu).

[By the way, the August 1989 issue of the Communications of the ACM has a set of papers from CPSR's Directions and Implications of Advanced Computing (DIAC) symposia, guest edited by Doug Schuler and Jon Jacky. PGN]

---

### **New Yorker Article on EMF Risks**

*Gordon Hester <[gh0t+@andrew.cmu.edu](mailto:gh0t+@andrew.cmu.edu)>*

*Fri, 28 Jul 89 18:38:13 -0400 (EDT)*

I have received numerous e-mail responses, as well as the ones that have appeared in Risks Digest, to my posting on Paul Brodeur's articles on electromagnetic fields (EMF) health risks in the New Yorker. I am forwarding this message to those who have asked for additional information; references to published sources on the subject appear at the end of it. My apologies to anyone who feels that I have not responded adequately to their requests. Please send me mail and I will try to respond, but I simply do not have time to respond individually to all of the mail I have already received.

First, several people have quite correctly taken me to task for calling Brodeur's use of the term "radiation" in his article titles "a complete misnomer." You are all correct: technically speaking, EMF is a form of radiation. My point, which I obviously did not make clearly, is that the use of this term will create an association in the minds of readers who are neither scientists nor particularly well-informed about radiation (and I feel confident that that includes virtually all regular readers of The New Yorker) to atomic or ionizing radiation. Public fear of atomic radiation and nuclear power is well known (and I say this without intending to make any judgment about whether that fear is justified, as that is irrelevant to the issue of EMF). I feel fully justified in characterizing Brodeur's use of the term radiation as misleading; it is one of many instances where he gives information that is in itself correct but that, due to a failure to include additional information, will tend to lead many readers to draw conclusions that are not justified.

I was considerably more disturbed by Jan Wolitzky's response to my comments on Brodeur's articles, and would like to respond in some detail to his criticisms. I find it very ironic that he chose not to respond to my point that Brodeur incorrectly assumes that researchers who have done studies that have yielded negative results on EMF health effects (that is, the results of which have been inconsistent with hypotheses that some such effects exist) have "cooked" their data to suit the preferences of their industry or government funding sources. Nevertheless, he accuses those of us who are working on this issue of doing exactly that!

In describing a booklet on EMF risks prepared by my colleagues here at Carnegie Mellon University, Wolitzky claims to have found "in the fine print in the front of the booklet" information that our research is supported by, and the production costs are paid for, the Electric Power Research Institute (EPRI). He asserts that this is the reason we are "go[ing] to such lengths to try to dampen public interest in the health effects of EMF."

Wolitzky omits other information that also appears on the first page of the booklet: that our research is also sponsored by the U.S. Department of Energy and the National Science Foundation, that preparation of the booklet (distinct from production costs) was supported by NSF, and that EPRI has NOT reviewed or approved the contents of the booklet. (They have, of course, seen it since it was produced.) This information is obviously relevant. By the way, the booklet is available from the Department of Engineering and Public Policy, Carnegie Mellon University, Pittsburgh, PA 15213. there is a charge of \$3.00 to defray production and mailing costs. (The funds EPRI provided for production are not separate from the research money we have; we charge this amount only to cover costs and do not make any profit. This is definitely NOT a commercial solicitation.) The booklet is titled "Electric and Magnetic Fields from 60 Hertz Electric Power: What do we know about possible health risks?" It is 45 pages long. It was produced, by the way, primarily for use in research on communicating to the public about this issue. It is being made generally available only because there is a paucity of information on the subject written in a way that is accessible to the public.

Wolitzky also writes of the booklet, "It also tries to discount epidemiological data that establishes a correlation between ELF [extremely

low frequency] radiation and cancers and birth defects, by saying that just because a rooster crows in the morning when the temperature is rising doesn't mean that the rooster CAUSED the temperature to rise." This is simply a distortion. This analogy is used in the booklet to explain the difference between establishing correlation and establishing causation, but the booklet does not try to discount the cause for concern created by the existence of positive epidemiological studies. It does show results from nine epidemiological studies of cancer, four of which are positive (i.e., the 95% confidence intervals fall entirely above the level of no change in cancer risk).

Finally, Wolitzky characterizes the group of researchers at Carnegie Mellon as trying to "lobby the public that there's nothing to get excited about here, that scientists don't all agree on the interpretation of the data, and that therefore we should follow a "prudent" course (they use that word a lot), by which they mean no government regulation at all, just maybe you should put your electric blanket on the shelf in the closet." There are four points here, which I will respond to in the order presented.

First, no one at CMU is trying to lobby the public. We are researchers, not politicians. We have made no attempt to widely distribute information to the public. We do, of course, provide information to research subjects who are drawn from the general population, both as part of our research and after their participation in that research. It is our responsibility as scientists to do this; it is also required by our university's policy and by generally accepted standards of scientific organizations. We also publish results of our research. Our publications sometimes appear in journals whose audiences include policymakers, but I don't think it would be accurate to describe this as "lobbying the public" by any means. Second, we do not characterize the possibility of EMF health risks as "nothing to get excited about." If we believed this, we wouldn't be interested in doing research in this area in the first place. I think it is fair to say that each of us currently is of the opinion that a conclusion that there definitely are health risks from EMF is not justified by the scientific evidence, although our opinions are individually held and I cannot presume to speak for my colleagues. In the booklet referred to here, which is the responsibility of M. Granger Morgan (others, including me, acted as advisors), the following appears under the heading "Do 60 Hz fields pose health risks?" "The honest answer is that nobody knows for sure. Scientists have found that fields can produce a variety of biological effects, like changes in the levels of specific chemicals the body makes and changes in the functioning of individual nerve cells and the nervous system. Whether any of these changes lead to health risks is less clear." In my opinion, this is a fair statement of the facts. However, it certainly does not mean that there is no cause for concern on the part of the public, government, researchers, or the utility industry. To the contrary, the scientific evidence now available is certainly cause for concern on the part of each of these groups.

Third, it is a FACT that scientists don't agree on how the currently available data should be interpreted. In his articles, Brodeur quotes the few people who are willing to conclude that there definitely is a health risk extensively - though I would not accept that those people as responsible scientists, any more than I would those who are now willing to conclude that there definitely is not

a health risk. It is notable, however, that Brodeur does NOT have any quotes from some of the quite responsible scientists he refers to in his articles to the effect that there definitely are significant public health risks - Ross Adey and Nancy Wirtheimer are the two examples that come to my mind. These people do say, and quite justifiably, that there is now cause for concern and for a concerted effort at doing more and better research - as do many other scientists. But that is not to say that they agree on how to interpret the available data.

Fourth, it is true that the booklet advocates a "prudent" course of action, and devotes some consideration to what is prudent. One thing that seems like it would probably be prudent for most people is to not use electric blankets, or at least not sleep under them. Another is to not sleep with your head near an electric clock that is motor driven - even small electric motors produce fairly strong magnetic fields. These are, clearly, actions that can be taken at an individual level, and at minimal cost. But large-scale societal action is not prudent at this time, given the uncertainty about whether there are any health effects from EMF and the possible extent of effects that may occur, for two reasons. First, the public expenditures that might be required are potentially enormous. It is not prudent to undertake those expenditures, which might accomplish literally nothing beneficial, when there are many other public health risks that are known to exist for which resources could be used and used effectively. Second, even if we were willing to take drastic measures, it is not clear what measures would be effective. The currently available evidence is not sufficient to give a clear indication of the measures of EMF exposure, if any, that are biologically effective and potentially pose health risks. (For example, the appropriate measure might involve time-averaged field strength, magnetic but not electric fields or vice versa, the specific wave form of the fields, the peak strength of the fields, or even exposure only to fields of specific intensities and frequencies and no others.) For exactly this reason, government regulation cannot be undertaken at this time with any confidence that it will be effective in reducing public health effects, even if one is willing to assume that such effects exist. It is quite conceivable that government regulations that arbitrarily limit field strengths (and such limits would necessarily be arbitrary, at least with respect to the potential for health effects) would actually INCREASE any public health effects that do exist. (Several states have nevertheless adopted such limits.) There is one action that government can undertake that would definitely be prudent, and those of us at CMU who are working on this problem advocate it strongly. That is to support further research. Unfortunately, it is the case that government support in this area has been declining rather than increasing over the last few years.

Now for some references:

1. Biological effects of power frequency electric and magnetic fields - background paper. Published by the Office of Technology Assessment, U.S. Congress. 1989. 103 pages. This is a fairly accessible summary of the EMF health effects literature. It also discusses policy issues, regulatory activity, and research programs briefly. Let me "warn" you that this report was prepared by my colleagues here at CMU, though they were commissioned by OTA. If you view us as a biased group, I guess you will have to look elsewhere. Available from gov't printing office, stock #052-003-01152-2, price \$4.75. 202-783-3238.

2. Electrical and biological effects of transmission lines: a review. Focuses on transmission lines, as the title implies. Prepared by staff of the Bonneville Power Administration, U.S. Department of Energy, Portland, Oregon 97208. 1986.

3. Biological and human health effects of extremely low frequency electromagnetic fields. Prepared by American Institute of Biological Sciences, 1985. Commissioned by the U.S. Navy. Disparaged in the Brodeur articles, by the way. Available from NTIS as Report # AD/A152 731.

4. Electromagnetic fields: cell membrane amplification and cancer promotion. By W. Ross Adey. Review paper presented at the National Council on Radiation Protection and Measurements Annual Meeting, National Academy of Sciences (Washington DC, 20418). 1986. A quite technical review of the scientific literature on cellular-level studies of EMF effects. I presume it is available from the Academy.

5. Biological effects of power line fields. Technical report prepared for the New York State Power Lines Project (also disparaged by Brodeur). NYSPLP, Wadsworth Labs, E-297, Empire State Plaza, Albany, NY. 1987.

These are the most recent reviews available, and I think they are from a wide variety of sources. If I knew of a source that in some way represented the view that EMF exposure definitely causes health effects I would provide it, but I don't. For specific papers, articles, etc., please see the bibliographies in the above sources.

Gordon Hester, Department of Engineering and Public Policy  
Carnegie Mellon University, Pittsburgh, PA 15213

[See also the collection of comments on this subject in [RISKS-9.10](#). PGN]

---

## **✉ Re: Gordon Hester on Paul Brodeur**

*Dan Schlitt <dan@sci.ccny.cuny.edu>  
Mon, 7 Aug 89 10:55:53 EDT*

I have watched with interest the discussion of the biological effects of low frequency electromagnetic radiation although I have not followed it in great detail or done research in the area. I have been a participant in the nuclear power safety debate and I find certain similarities in both the content and the players. [...]

While I expect that the objection to the use of the term "radiation" in this case is basically a public relations objection, there is a possible real distinction to be made. For the low frequency fields much of the exposure occurs in the near field region. The fastidious might wish to limit the use of the term "radiation" to the far field region.

Since I am more impressed by mechanistic explanations than I am by statistical epidemiological evidence, I am willing to believe that the

differences in field configuration in the two regions may cause different biological effects.

>There seems to be a concerted effort on the part of the Dept. of Engineering  
>and Public Policy at CMU to lobby the public that there's nothing to get  
>excited about here, that scientists don't all agree on the interpretation of  
>the data and that therefore we should follow a "prudent" course (they use that  
>word a lot), by which they mean no government regulation at all, just maybe you  
>should put your electric blanket back on the shelf in the closet.

This is what I have come to expect of this group at CMU. My own feeling about prudence is that exposure should be minimized in the face of uncertainty about safety. However I think that this can be taken too far. Wide right-of-ways under high voltage transmission lines seem reasonable to me. But I'm not going to get too excited about the effects of electric blankets. (But then, I don't use the things.)

BTW, don't be fooled by the signature. I am a theoretical physicist by training and spent twenty-some years of my life on the faculty of physics at a large state university.

Dan Schlitt, Manager, Science Division Computer Facility,  
City College of New York, New York, NY 10031 (212)690-6868



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 9: Issue 12

Thursday 17 August 1989

## Contents

- [RISKS IS FINALLY MOVING TO CSL.SRI.COM!](#)  
[PGN](#)
- [Flaws in calculations, computer models in Trident failures](#)  
[Jon Jacky](#)
- [Voyager 2 software faults at launch, 1977 Aug 20 10:29](#)  
[David B. Benson](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✉ RISKS IS FINALLY MOVING TO CSL.SRI.COM!

*Peter G. Neumann <Neumann@KL.SRI.COM>*

*Thu, 17 Aug 89 09:07:12 PDT*

This should be the last issue of RISKS that you will receive from the KL. Subsequent issues should appear without interruption from the CSL. As has already been noted in the masthead for many months, all RISKS mail should be directed to [RISKS@CSL.SRI.COM](mailto:RISKS@CSL.SRI.COM) or [RISKS-Request@CSL.SRI.COM](mailto:RISKS-Request@CSL.SRI.COM), depending on whether you have a contribution or an out-of-band message, respectively. Please send mail to the latter address ONLY IF YOU DO NOT RECEIVE a message from [RISKS@CSL.SRI.COM](mailto:RISKS@CSL.SRI.COM) within 24 hours of your receiving this issue. That message from CSL will be identified by

"From RISKS Forum <[RISKS@CSL.SRI.COM](mailto:RISKS@CSL.SRI.COM)>

Subject: RISKS IS NOW ABOUT TO MOVE. NO ACK REQUIRED IF YOU RECEIVE THIS."

[The DEC 2065 and its staff have been very good to RISKS for the past four years. Many thanks to Steve Milunovic for all his help. PGN]

---

### ✉ Flaws in calculations, computer models implicated in Trident failures

*Jonathan Jacky, University of Washington <[JON@GAFFER.RAD.WASHINGTON.EDU](mailto:JON@GAFFER.RAD.WASHINGTON.EDU)>*

*Thu, 17 Aug 1989 9:21:56 PDT*

Here are excerpts from a story that appeared on the front page of the Thursday, August 17, 1989 NEW YORK TIMES:

DESIGN FLAW SEEN AS FAILURE CAUSE IN TRIDENT 2 TESTS --- by Andrew Rosenthal

WASHINGTON --- The Navy believes designers made a fundamental miscalculation in building its biggest nuclear missile, the Trident 2, which has failed in two of its three undersea tests, a Navy official said yesterday.

The first missile exploded on March 21, four seconds after it was launched from a submarine off the east coast of Florida. The second test, on August 2, went largely according to plan, but the third blew up Tuesday.

Rear Adm. Kenneth C. Malley, head of the Navy's ballistic missile program, said that despite computer simulations, engineers seriously underestimated how much pressure is on the Trident 2 as it hurtles up through the water from its submarine launcher. He said they had also failed to anticipate the effect of "water jets" caused by the missile's movement. ...

The Trident 2, which is 44 feet long and weighs 130,000 pounds at launching, is much longer and nearly twice as heavy as the Trident 1 [...which is now in service and which Trident 2 is scheduled to replace...]. Although engineers expected the larger missile to create more turbulence than the Trident 1 as it passed through the water, they miscalculated how much more and what effect that would have on the Trident 2's rocket engines. ... During testing "water jets" caused by the missile's movement contributed to the turbulence. After reviewing the tests of the Trident 1, the Navy said, such jets were present, but had gone unnoticed because they had not affected the smaller missile's flight. ...

The first time the missile was tested at sea, Admiral Malley said, the unexpectedly strong pounding from the water jet caused the (missile's rocket) nozzles to malfunction as soon as they fired above the water's surface. The missile began spinning in a spectacular cartwheel until it self-destructed. ...

In the third test, ... instead of spinning end-over-end, (the missile) began flying on what at first seemed to be a normal trajectory ... "Then it appeared to be losing some thrust control and it self-destructed." Admiral Malley said he had not yet studied the full body of data from the test. But he said it appeared that the aft-end pressure had severed electrical connections...

Asked whether the failures were a result of a design error or of a flaw in manufacturing that left the rocket weaker than it should have been, Admiral Malley said, "The device was built to specification. There is no question that it was designed the way it was intended to be designed."

As a result of the miscalculation, Malley said in an interview, the original nozzles on the missile's first-stage rocket were not strong enough to withstand the additional turbulence, and they had to be redesigned after the first test missile exploded. The Navy now must go back to the laboratories to determine why the rebuilt nozzles failed Tuesday, Malley said. ...

Until the test failures, the Trident 2 was the one element of the Defense Department's nuclear modernization program that was moving along smoothly,

having successfully completed 16 of 19 test firings from land...

Because there are so many Navy officials and subcontractors involved in the Trident 2 program, it is impossible at this point to assess when or by whom the miscalculations were made. The prime contractor is Lockheed Corp. ...

---

### **✂ Voyager 2 software faults at launch, 1977 Aug 20 10:29**

*David B. Benson <dbenson@cs2.WSU.EDU>*

*Wed, 16 Aug 89 12:35:15 PDT*

Exerpts from: "Voyager and the Grandest Tour Ever: Catching the Wave of the Century", by Bruce Murray, California Institute of Technology's <Engineering & Science>, Summer 1989, (no volume number). This article is itself excerpted from "Journey into Space: The First Three Decades of Space Expolration", by Bruce C. Murray, publ. W.W.Norton & Co., 1989.

[Except for inadvertent typos, the following is an exact quotation from the article, including the misused quotation marks. I shall refrain from other remarks, leaving such to our Gentle Editor.]

...

Voyager 2's gyroscopes and electronic brain were alive during the Titan/Centaur launch, monitoring the sequence of events in order to take control upon separation. But here the unexpected happened: Voyager 2's brain experienced robotic "vertigo." In its confusion, it helplessly switched to backup sensors, presuming its "senses" to be defective. Still no relief from its disorientation. Mercifully, the panicky robot brain remained disconnected from Voyager's powerful thrusters, so it did not cause damage to the launch. The Centaur attitude-control system -- under its normally behaving brain -- stayed in charge, suffering no "vertigo" and, as planned, electronically correcting the disequilibrium of Voyager's brain just before separation.

From the control center John Casani and his terse engineers helplessly watched (though mostly they listened, because there were not enough monitors available to us in Florida) the antics of Voyager 2's disoriented brain. One hour and 11 minutes after lift-off, Voyager 2 fired for 45 seconds its own special solid rocket to provide the final push it needed to get to Jupiter.

One and a half minutes after Voyager's key rocket burn ended, a ten-foot arm holding the television camera and other remote-sensing instruments was unlatched and deployed as planned. Then, more trouble. Voyager's anxious brain once again sensed an emergency. This time it switched thrusters and actuated valves to control the tiny bursts of gas used to stabilize its orientation. Voyager's robotic "alter ego" (its executive program) then challenged portions of its own brain in a frantic attempt to correct the orientation failure it sensed. Next, Voyager followed the procedures JPL engineers had installed to cope with the most dreaded emergency for a robot in deep space -- spacecraft attitude disorientation. (In August 1988 the Phobos 1 spacecraft of the Soviet Union succumbed to such an emergency after receiving an erroneous ground command, and in March 1989 Phobos 2 evidently met a

similar fate.) Voyager shut down most communications with Earth in order to begin its reorientation.

Seventy-nine minutes passed while Voyager 2 struggled alone and unaided to find the sun and establish a known orientation. Finally, it radioed confirming data. For the moment, Voyager 2 was stable.

It was all work and no celebration that afternoon in the dimly lit High Bay Conference Room, where, just days earlier, a seemingly healthy Voyager 2 had checked out perfectly. Were the redundant sensors malfunctioning? Was the state-of-the-art brain defective?

The technical discussion in the room was poorly illuminated too. All the new, supersophisticated fault protection in Voyager's electronic brain operated on the now-painful presumption that it would be triggered <only> by a hardware failure billions of miles from Earth. In that event Voyager would be unable to establish even emergency communications with its human handlers, who could not help it much at that distance in any case. As a consequence Voyager had been programmed virtually to shut off communications with Earth during such emergencies and to fix itself. But, somehow, these deep-space procedures had been triggered right after the launch.

Now, because of those disrupted communications, we were not receiving the useful flow of engineering-status measurements. We simply lacked enough information to figure out the causes of Voyager's mysterious behavior, even though the spacecraft was so close to Earth that communications normally would have been feasible under any emergency.

...

... There had been no hardware problems in the brain -- just a slight but serious missetting of computer parameters.

...



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

**Volume 9: Issue 13**

**Friday 18 August 1989**

## Contents

- [Phony IRS refunds by computer](#)  
[Rob Gross](#)
- [Cellular phones in stings](#)  
[David Wittenberg](#)
- [Aircrew acceptance of flight automation](#)  
[Robert Dorsett](#)
- [Unauthorized Internet activity](#)  
[CERT Internet Advisory -- Kenneth R. van Wyk](#)
- [Re: Marijuana virus wreaks havoc in Australian Defence Department](#)  
[Anthony John Apted](#)
- [More on the Wily Hackers](#)  
[Rob Gross](#)
- [Training and Software Engineers](#)  
[Tim Shimeall](#)
- [Computer-based airline ticket scam](#)  
[Jordan Brown](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **✂ Phony IRS refunds by computer**

*Rob Gross* <<GROSS@BCVMS.BITNET<>

*Thu, 17 Aug 89 20:59 EST*

Computer filer got \$325,000 in phony refunds, IRS claims

John King, Globe Staff

(Boston Globe of Thursday, August 17)

Clever tax preparers are one thing, but a clever bookkeeper who allegedly pried 325,000 dollars from the Internal Revenue Service found himself on the wrong side of the law yesterday.

In what may be the nation's first charge of electronic tax fraud, IRS special agents yesterday arrested Alan N. Scott of West Roxbury [a part of Boston], saying he claimed 45 fraudulent income tax refunds for amounts

ranging from 3,000 dollars to 23,000 dollars.

The IRS charges that Scott, 37, used the service's new electronic filing system -- open only to tax preparers -- to submit phony claims with assumed names and Social Security numbers. In some cases, the names used were of people in prison, according to Chief Kenneth Claunch, IRS Criminal Investigation Division.

"The computer age has spawned a new breed of criminal," Claunch said in a statement.

New in tools, perhaps. As for the basic idea -- filing a false return in order to snare an unwarranted refund -- that's old hat, admitted IRS spokeswoman Marti Melecio.

"I can't say that it's a new trick. We've had fraud cases with paper returns," Melecio said. "The time frame is different, though. With electronic filings, the returns come back in two or three weeks."

According to the IRS, Scott received electronic filing status on Jan. 31. He did this by using a false Social Security number, and making false statements on his application. However, the IRS also says Scott electronically filed 10 returns where he used his own name as a preparer, and these returns appear to be legitimate.

The scheme was uncovered by the a [sic] "questionable refund detection team," at the IRS service center in Andover [Massachusetts]. Also, the IRS credited a tip from an unnamed boston bank "which reported a suspicious electronic transfer of funds to an individual," presumably Lewis [sic].

If convicted, Lewis [sic] faces a possible prison sentence and up to 250,000 dollars in fines on each of the counts of fraud.

---

### Cellular phones in stings

*David 'Witt' DTN 293-5071 <wittenberg%ultra.DEC@src.dec.com>  
Wed, 16 Aug 89 07:03:24 PDT*

In Friday's (11 Aug) Wall Street Journal, there was an article on cellular telephones. Of particular interest was the discussion of using cellular phones to replace two way radio in police departments in "sting" operations. It seems that the people they were chasing listened to police band scanners and were evading the police, so the police switched to cellular telephones to maintain secrecy.

I'm not sure if I'm more touched or scared by such misplaced faith in a new technology. (The lack of secrecy in cellular phones has been discussed at length in this forum.)

--David Wittenberg

---

## **✈ Aircrew acceptance of flight automation**

Robert Dorsett <rd@rascal.ics.UTEXAS.EDU>

Thu, 17 Aug 89 22:25:03 CDT

The August 7 issue of *Aviation Week and Space Technology* has a feature story on how well flight automation has been received by aircrews. Earl Wiener (co-editor of *Human Factors in Aviation*, in which similar stats were revealed) has released the results of a survey of some 200 757 pilots. The data shows strikingly opposed opinions--either the pilots love the automated systems, or they hate them.

The article mentions one problem, which hasn't gotten much press attention, is that the automated systems encourage a "heads-down" atmosphere under 10,000'. The UI's are apparently so bad that a single pilot must devote all his attention to updating and manipulating information in their flight management and control control systems (FMCS), in effect reducing the cockpit to single-pilot operation for substantial periods.

The article also mentions identification of various problems that need attention:

"\* Further reduction of workload in low-workload phases of flight caused by automation (for example, long haul over water.

\* Further increase in workload in high-workload phases of flight caused by automation (for example, terminal area).

\* A potential for substantially increased "head-down" time.

\* Difficulty in recovering from automation failure.

\* Reluctance of flight crews to take over a malfunctioning automated system.

\* Deterioration of pilot/controller basic skills.

\* Complacency, lack of vigilance and boredom in workers.

\* Introduction of unanticipated failure modes.

\* Incompatibility between advanced automated aircraft, existing air traffic control capability and the rest of the fleet."

The article also notes some fairly critical UI problems:

"Pilots even work around aspects of the computer program that do[es] not provide the desired performance. For example, crews who want to start vertical navigation descents earlier than the computed top-of-descent point simply tell the computer they plan to use anti-ice when, in fact, they do not, or they program in a fictitious tail wind. The computer then refigures a new top-of-descent point to the pilot's liking. This procedure is often needed because the Boeing 757, considered an aerodynamically stable aircraft, does not descend as readily as earlier models. Pilots like to avoid using speed brakes to conserve fuel and avoid disturbing passengers."

It's interesting to note that Wiener wishes to solve the automation problem by imposing a greater level of automation (the article is fairly vague about what he has in mind--my interpretation is a combination of higher-level services and better-designed user interfaces).

The article doesn't treat cockpits utilizing unconventional control laws, such as those the A320's fly-by-wire system utilizes (but otherwise, A320 flight management principles are quite similar to the systems utilized elsewhere).

Some comments and opinions:

The problems at altitudes less than 10,000' are quite interesting. Automation has generally been marketed as a "workload-saving" item. Particularly after the midair collision between a PSA 727 and a Cessna 172 in 1978, simplified cockpits, and consequent automation, was marketed as a means of keeping the pilots' eyes looking out of the airplane. In effect, however, the basic problem is unsolved (if, indeed, it was a problem, which is another story). Automation has done *\*nothing\** to simplify the actual tasks of *\*flying\** the airplane: the older autopilots, with heading, altitude, and airspeed select, were excellent aids to operating in control environments. The key in the current problems seems to be in the flight management control system, which first started entering widespread use in 1982-83. The idea behind the FMCS was that it could be programmed with economical flight profiles, and then be coupled to the autopilot, thus creating a highly economical flight. Comments in the Aviation Week article (which, incidentally, runs counter to the gung-ho attitudes in similar technology reviews in Flying and Flight International) suggest that pilots are not utilizing the system, and that the system itself is not selecting the most optimal flight characteristics. In effect, they appear to be reverting to manual manipulation of the autoqtpilot.

Robert Dorsett      UUCP: ...cs.utexas.edu!rascal.ics.utexas.edu!rdd

---

### **✂ CERT Internet Security Advisory -- unauthorized Internet activity**

*Kenneth R. van Wyk <krvw@SEI.CMU.EDU>*

*Wed, 16 Aug 89 11:50:22 EDT*

Many computers connected to the Internet have recently experienced unauthorized system activity. Investigation shows that the activity has occurred for several months and is spreading. Several UNIX computers have had their "telnet" programs illicitly replaced with versions of "telnet" which log outgoing login sessions (including usernames and passwords to remote systems). It appears that access has been gained to many of the machines which have appeared in some of these session logs. (As a first step, frequent telnet users should change their passwords immediately.) While there is no cause for panic, there are a number of things that system administrators can do to detect whether the security on their machines has been compromised using this approach and to tighten security on their systems where necessary. At a minimum, all UNIX site administrators should do the following:

o Test telnet for unauthorized changes by using the UNIX "strings" command to search for path/filenames of possible log files. Affected sites have noticed that their telnet programs were logging information in user accounts under directory names such as "... " and ".mail".

In general, we suggest that site administrators be attentive to configuration management issues. These include the following:

o Test authenticity of critical programs - Any program with access to the network (e.g., the TCP/IP suite) or with access to usernames and passwords should be periodically tested for unauthorized changes. Such a test can be done by comparing checksums of on-line copies of these programs to checksums of original copies. (Checksums can be calculated with the UNIX "sum" command.) Alternatively, these programs can be periodically reloaded from original tapes.

o Privileged programs - Programs that grant privileges to users (e.g., setuid root programs/shells in UNIX) can be exploited to gain unrestricted access to systems. System administrators should watch for such programs being placed in places such as /tmp and /usr/tmp (on UNIX systems). A common malicious practice is to place a setuid shell (sh or csh) in the /tmp directory, thus creating a "back door" whereby any user can gain privileged system access.

o Monitor system logs - System access logs should be periodically scanned (e.g., via UNIX "last" command) for suspicious or unlikely system activity.

o Terminal servers - Terminal servers with unrestricted network access (that is, terminal servers which allow users to connect to and from any system on the Internet) are frequently used to camouflage network connections, making it difficult to track unauthorized activity. Most popular terminal servers can be configured to restrict network access to and from local hosts.

o Passwords - Guest accounts and accounts with trivial passwords (e.g., username=password, password=none) are common targets. System administrators should make sure that all accounts are password protected and encourage users to use acceptable passwords as well as to change their passwords periodically, as a general practice. For more information on passwords, see Federal Information Processing Standard Publication (FIPS PUB) 112, available from the National Technical Information Service, U.S. Department of Commerce, Springfield, VA 22161.

o Anonymous file transfer - Unrestricted file transfer access to a system can be exploited to obtain sensitive files such as the UNIX /etc/passwd file. If used, TFTP (Trivial File Transfer Protocol - which requires no username/password authentication) should always be configured to run as a non-privileged user and "chroot" to a file structure where the remote user cannot transfer the system /etc/passwd file. Anonymous FTP, too, should not allow the remote user to access this file, or any other critical system file. Configuring these

facilities to "chroot" limits file access to a localized directory structure.

- o Apply fixes - Many of the old "holes" in UNIX have been closed. Check with your vendor and install all of the latest fixes.

If system administrators do discover any unauthorized system activity, they are urged to contact the Computer Emergency Response Team (CERT).

Kenneth R. van Wyk, Computer Emergency Response Team cert@SEI.CMU.EDU  
(412) 268-7090 (24 hour hotline)

---

## **✦ Re: Marijuana virus wreaks havoc in Australian Defence Department**

*Anthony John Apted <Apted@DOCKMASTER.NCSC.MIL>  
Tue, 15 Aug 89 14:43 EDT*

I am aware of the RISKS attitude to redundancy, however I would like to present an Australian viewpoint on this incident. (see [RISKS 9.9](#))

First, some background. I have worked for the Australian Defence Dept. for six and a half years: five and a half as a programmer/analyst on real-time systems, and twelve months in Computer Security. I am currently on a twelve-month posting with the NCSC, gaining experience in software verification.

The following newspaper article arrived in the mail from home yesterday. It is from the Melbourne 'Sun News-Pictorial', dated 8/8/89.

"Terminal virus rocks defence" by George Megalogenis.

"Australia's Defence Department has been bugged by a computer virus posing as a messenger for an illicit drug.

Confused staff where [sic] greeted with the message: 'Your machine has been stoned - Legalise marijuana' when they tried to operate infected terminals last week.

A spokesman confirmed yesterday that eight high-security terminals in Canberra came down with the bug.

The defence bug was reported as having destroyed sensitive departmental data.

The department is remaining tight-lipped on the source of the infection as it does not want to encourage computer hackers to pull similar stunts.

A computer virus begins life as an innocent program on a particular terminal.

But a hacker can use it to cause mischief by spreading the unwanted or false information to other terminals and systems.

The programmer can also direct the virus to destroy existing files.

The department spokesman said the technical virus had been 'isolated and the computers decontaminated'.

The spokesman said he could not rule out the possibility that the virus was created by accident.

The department was working on programs designed to weed out future

intruders before they caused any damage, he said."

A few remarks on the preceding:

Ignoring (for the moment) the quality of the article: I am not surprised "the department is remaining tight-lipped"; based on my knowledge of the department, and of similar occurrences in other government organisations, the most likely explanation for the appearance of the virus on Defence PCs is that someone brought into the office their own infected floppies, probably to play games. This sort of thing is not looked on kindly by the Department (to put it mildly).

[The [RISKS 9.9](#) posting suggested that the office, involved in virus/anti-virus research, might have had an internal accident: certainly possible - eight machines infected smacks of carelessness, but obviously someone was, somewhere along the line, whatever the actual cause.]

Now to the quality of the article: this is (fairly obviously) an appalling piece of reportage - lack of technical knowledge on the part of the writer (and sub-editor) is quite evident in (among other things) the persistent use of the word "terminal" instead of "personal computer", and the amazing statement that "A computer virus begins life as an innocent program...".

It is acknowledged that the 'Sun' is not the highest quality newspaper in Australia - nevertheless it is not a typical tabloid-style either. Therefore, I personally find the lack of quality of information in this article disturbing (especially as the 'Sun' had given good-quality reporting and commentary on the Internet worm).

The main RISK? the 'Sun' is the highest circulation paper in Victoria, if not Australia [approx. 650,000 daily]; its readership is typically blue-collar and secretarial/clerical type people - those most likely to be naive users of personal computers, and most likely to be influenced by (i.e. believe verbatim) the contents of this article.

Anthony J. Apted

DISCLAIMER: Any original thoughts expressed in the above are my own, and do not represent the views of either the Australian or American governments (any unoriginal thoughts are the responsibility of their owners).

---

### More on the Wily Hackers

*Rob Gross <<GROSS@BCVMS.BITNET>>  
Thu, 17 Aug 89 20:59 EST*

W. German computer hackers accused of spying for Soviets  
(Boston Globe of Thursday, August 17)

Associated Press (Frankfurt) --- Three computer hackers, suspected of giving the Soviet Union information from military and industrial computers worldwide,

have been indicted on espionage charges, prosecutors said yesterday. The West German government called the breakup of the spy ring, which gave the KGB secret data from 12 countries, including the United States, "a major blow" to the Soviets. In a four-page statement, Kurt Rebman, the chief federal prosecutor, said it was the first time his office had prosecuted hackers for endangering national security.

[See [RISKS-9.34](#) for the earlier background on the Wily Hackers. PGN]

---

## ✂ Training and Software Engineers (was: UK Defence Software Standards)

*Tim Shimeall x2509 <shimeall@cs.nps.navy.mil>*

*Thu, 3 Aug 89 09:39:52 PDT*

Another message in the thread of comments from my friend (replies to me for relaying, or to RISKS). Tim

Douglas W. Jones states that the terms software engineering and software engineer have gotten out of control. He is correct, but it seems to me that his solution, to regulate the use of the title "software engineer", is a rather weak one.

In his comment, he gives a general outline of a set of standards that have been suggested to restrict the use of the term engineer, and suggests that some similar approach might be used:

- > 1) People who have passed a state professional engineering examination.
- >
- > 2) People who have graduated from an accredited 4-year engineering program.
- >
- > 3) People who have graduate degrees.

The problem with regulating the term is that it does not regulate the work that the individual does. In my last comment, I mentioned that I have worked with people who had A.A. degrees or were merely high school graduates who were called "software engineers". What I should probably have made clearer is that it is not simply that they call themselves that; it is what they are called by their employers. They will be doing the same work, with or without the title, as long as they continue to work for those employers.

Software engineering, even compared to electrical engineering is a very young discipline. While I would meet the second of the criteria he lists, most of the professors I studied under to get the degree would not. As a group, their doctorates were in areas ranging from Physics to English, with only the younger members of the department having degrees in Computer Science.

Software engineering is still very much in its infancy. There are several basic rules that derive from this fact:

- 1) Acceptable levels of knowledge and techniques for today will not be acceptable tomorrow.

- 2) There are not enough "real" software engineers available to do the work that requires their services.
- 3) There are a lot of people out there who call themselves software engineers who are not "real".

An engineer, as defined by the firm I happen to work for now, is someone with a degree in an engineering discipline from a school with a recognized engineering department. A software engineer is an engineer who writes software, as opposed to a computer programmer who is a non-engineer who writes software. The two may work side-by-side on exactly the same task, doing exactly the same thing, but that is the only difference. Who gets assigned to what task is largely dictated by what the previous experience of the person is, not job title. This is in a large aerospace firm.

An engineer, as defined by the last place I worked for, was someone with a certain minimum level of experience who worked overtime for free. The degree was accepted in lieu of that minimum level of experience, but that was about the only difference. The two people, one degreed, one not may work side-by-side on exactly the same task, doing exactly the same thing, with exactly the same job title. Who gets assigned to what task is largely dictated by what the previous experience of the person is, not degree status. This is not a large aerospace firm, but how different is it really?

Is the fact that the software engineer got a degree 29 years ago in electrical engineering that significant to his job function? Many of the professors I studied under when I got my own degree had their degrees in areas unrelated to computer science.

One of the most reliable (in terms of safe and effective product) "software engineers" I had the pleasure of working with in the past is not degreed. He learned his trade by the apprenticeship method, still one of the most reliable methods. He spent a great deal of time and effort in understanding the application area in which he worked, and the effort showed. One of the least reliable "software engineers" I worked with went to great lengths to make sure we all know he had a MS in Software Engineering from a good technical school. He was ultimately laid off because of the terrible quality of the code he produced, and because he refused to learn from people who were academically "beneath" him.

it is unreasonable trying to regulate something that is not be possible to regulate. (Sure we can limit the use of the term, but can any agency actually place that stringent a limit on who actually does the work? When the people are simply not there to do it? Ask the INS about illegal aliens doing household chores and working in factories sometime.)

I feel that a far more effective solution at this time, is to attempt to communicate with the companies involved with RISKy projects (either building them, buying them, or using them) about the type of expertise needed for these projects, to develop a set of livable standards that take into account the level of expertise presently available in the general population of "software engineers" available in the field (as the MOD has tried to do), and to attempt to produce enough QUALIFIED people to meet the genuine need for them. In

this way, we have a livable (albeit painful) solution for the short term, and a reasonable hope for something better in the future.

---

### ✈ Computer-based airline ticket scam ([RISKS 9.11](#))

Jordan Brown <[jbrown@herron.UUCP](mailto:jbrown@herron.UUCP)>

Thu, 17 Aug 89 09:59:37 PDT

> From: Rodney Hoffman <[Hoffman.ElSegundo@Xerox.com](mailto:Hoffman.ElSegundo@Xerox.com)>  
> Investigators said the individuals put together a major conspiracy  
> by knowing how to access airline computers to put travel itineraries  
> in the computer system. ++++++

In the interests of equal access to scammy to all, I will divulge some of the deep secrets of how to access airline computers and insert travel itineraries. This can be done from virtually any telephone nationwide (even a dial phone!). The process is virtually immune to tracing if you use a public phone; your identity is protected.

First, it is necessary to determine the secret access code for the airline computer. To do this it is necessary to penetrate the telephone company's databases. Pick up the phone and dial 1-800-555-1212. This will connect you to a human-assisted database of access codes. Say (for instance) "American Airlines Reservations". The database system will read you a number, 800-433-7300.

Hang up and dial this number (probably prefixed by a 1). This will connect you to another human-assisted database which stores all of American Airlines' itineraries. Simply state the date, flight number, departure and destination cities, and passenger name. It's that easy! You can later dial the same access number and cancel or modify your itineraries. The system even includes search functions if you don't know the flight number, and an extensive help system (just say "How do I make a reservation?"). It's almost like they tried to make this sort of illicit use simple. Jordan Brown  
[jbrown@jato.jpl.nasa.gov](mailto:jbrown@jato.jpl.nasa.gov)

[Cute. But I suspect unauthorized on-line access might also be parlayed into other spin-offs, such as getting tickets issued without paying. 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 9: Issue 14**

**Monday 21 August 1989**

## Contents

- [The Check's in the Mail \(but the water got shut off anyway\)](#)  
[Dave Clayton](#)
- [Australian Commonwealth Bank -- doubled deposits](#)  
[Martyn Thomas](#)
- [Automatic vehicle navigation systems](#)  
[Pete Lucas](#)
- [Tired of computers being trusted? \(a balancing act for wheel watchers\)](#)  
[PGN](#)
- [Re: Computer-based airline ticket scam](#)  
[Jules d'Entremont](#)
- [Human failures in emergencies](#)  
[Henry Spencer](#)
- [Hazards of Airliner Computerization](#)  
[Mike Trout](#)
- [Re: California studies "drive-by-wire"](#)  
[John Chew](#)
- [First test for electronic tagging starts in jail!](#)  
[Olivier Crepin-Leblond](#)
- [Re: unauthorized Internet activity](#)  
[anonymous](#)
- [DEMO Software Disk Infected \(Jerusalem Version B\)](#)  
[J. Vavrina](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **✉ The Check's in the Mail--really (but the water got shut off anyway)**

*Dave Clayton* <[LCO101@URIACC.BITNET](mailto:LCO101@URIACC.BITNET)>

*Mon, 21 Aug 89 12:43:35 EDT*

WATER SHUT-OFFS NOT INTENTIONAL

(From The Daily Spectrum; St. George, Utah, serving millions of acres of slickrock and a few thousand people!)

Pleasant Grove, Utah(AP)

Pleasant Grove city officials say they have found and fixed the reason for several water users being cut off--despite having paid their bills.

An apologetic City Recorder Charmaine Childs explained that in June, Pleasant Grove switched to a new envelope bill, replacing the postcard billing it had used for years.

The new bills include an envelope for residents to mail their payments. What officials didn't realize, however, that the bar code printed on the

^^^^^^^^

envelope was for Orem rather than Pleasant Grove.

As the bar codes are read electronically by automated postal equipment,

^^^^ ^^^^^^^^^^^^^^^^^^^^ ^^ ^^^^^^^^^^^ ^^^^^^^ ^^^^^^^^^^^^

when residents mailed their water payments they went to Orem instead of Pleasant Grove.

Childs said the Pleasant Grove postmaster noticed the wrong bar code on some of the envelopes and asked postal employees to watch for the blue envelopes and route them to Pleasant Grove rather than Orem.

\* \* \* \* \*

(It gets thirsty out there on the desert without water.)

Dave Clayton, Academic Computing, U. of Rhode Island

---

### **Australian Commonwealth Bank -- doubled deposits**

*Martyn Thomas <mct@praxis.UUCP>*

*Mon, 21 Aug 89 12:11:36 BST*

This story appears in Datalink (UK Trade weekly) August 21st 1989. It contains no dates or references by which it can be checked.

"Some cock-ups are bigger than others. Some are little but some come in such gigantic proportions that they stretch credulity. Take, for example, the mishap that afflicted the Australian Commonwealth Bank's computer. One could imagine all sorts of things going wrong with such an installation which keeps the scores on thousands of customers. But it's hard to imagine what went wrong when a malfunction at the bank doubled every deposit that customers made. As DP manager Pete Martin says: 'Of course it's a cock-up, it's a vast bloody cock-up. The hazards of computing are only limited by your imagination.' "

Is this the story of mounting a transaction tape twice, previously reported (though I can't remember who the bank was), or is it a new story? Is it true?

-- Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK.

Tel: +44-225-444700. Email: ...!uunet!mcvax!ukc!praxis!mct

---

### **Automatic vehicle navigation systems**

*"Pete Lucas - NERC Computer Services U.K." <PJML@ibma.nerc-wallingford.ac.uk>*

*Mon, 21 Aug 89 09:48:20 BST*

I read with some interest the recent proposals for auto-pilot systems for passenger vehicles. I must confess, these fill me with horror. The thought of a systems failure on one or more such vehicles, and the inability of the others to do much about it, is my greatest worry. Call me a technophobe if you like, but *\*NOBODY\** can guarantee 100% reliability. The problems of power failures, parity errors, external magnetic/radio fields, poor maintenance etc. are as yet still serious considerations as to why such systems should not be implemented. Systems based on digitised street maps are never going to work - i can still remember being told by my brother, who was navigating me, 'Take a 90 right 50 yards after the farmhouse...' only to discover that the farmhouse had been demolished the week before... This caused great amusement to the wreckers who recovered the resultant wreck from the swamp and towed it back to civilisation. How an auto-navigation system manufacturer would explain this sort of problem when 100 card ended up in the swamp, i cannot imagine.

The fewer levels of 'indirection' in such systems the safer they become - to place a (semi-)intelligent control system between the driver and the vehicle is by definition reducing driver control (although having driven in the States this may be no bad thing!) and increasing the number of possible failure modes.

Two things to remember::

- 1) Keep It Simple, Stupid!
- 2) If you never depended on it, you can carry on without it.

Natural Environment Research Council, NERC Computer Services, Holbrook House,  
Station Road, SWINDON SN1 1DE

JANET: PJML@UK.AC.NERC-WALLINGFORD.IBMA      PHONE: +44 793 411613

---

### ***⚡ Tired of computers being trusted? (a balancing act for wheel watchers)***

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

*Sat, 19 Aug 1989 11:37:29 PDT*

Blind trust in computer systems struck home this week. My daughter brought her car off-island for the initial 7500-mile dealer checkup that included rotating and rebalancing the tires and checking the alignment. After the return ferry trip and drive home, she noticed a terrible shimmy and called the dealer to complain. The dealer claimed that they then determined that their computer had been malfunctioning, and apologized profusely. (Perhaps the mechanic was not sufficiently computer literate?) She immediately took the car to the best tire man on the island, who said he had NEVER seen anything so badly out of balance. (The dealer covered the cost.)

Are there no consistency checks or reasonableness checks on the results of such computerized systems? Are they designed to be mechanic-proof? Are we getting to the point that almost everyone in society is going to have to be not just computer literate, but keenly aware of the risks and pitfalls? Probably No, No, and Yes.

[I contemplated the plight of a land-locked driver having to negotiate such an ill-adjusted car when heavily laden, and came up with something about where the lubber meets the load. As I have been far too conservative in my interstitial insertions of late, I thought you wouldn't mind. PGN]

---

**✂ Re: Computer-based airline ticket scam ([RISKS 9.11](#))**

Jules d'Entremont <jules@iisat.UUCP>

20 Aug 89 00:42:27 ADT (Sun)

>From: Jordan Brown <jbrown@herron.UUCP>

>In the interests of equal access to scammy to all, I will divulge ...

It sounds like Jordan is, like me, growing tired of all these stories about "computer crime". What is computer crime anyway? Crime has existed since the dawn of civilization, and criminals have always been eager to use the latest technology for their sinister deeds. Guns, knives, cars, matches, even panty hose are used by criminals daily, but when is the last time you read a newspaper article about "panty hose crime?"

Crime is crime. It took a long time before the term "computer error" fell out of favour with most people; how much longer will it take for "computer crime" to reach the same fate?

Jules d'Entremont Phone: 454-5631 (Home) 465-5535 (Office)

UUCP: {uunet,utai,watmath}!dalcs!iisat!jules

Bitnet/Uucp: jules@iisat.uucp Arpanet: jules%iisat.uucp@uunet.uu.net

---

**✂ Human failures in emergencies**

<henry@utzoo.UUCP>

Mon, 21 Aug 89 01:30:47 -0400

The July 17 issue of Aviation Week has a very interesting letter from P.G. Boughton, commenting on the British 737 crash in which the pilot shut down the good engine instead of the bad one:

"I am amazed that Boeing has taken all the blame... I am an F-14/F-4 backseater with more than 3000 hr. Twice I have had experienced pilots shut down the incorrect engine. Both times we had enough airspeed and altitude to get the engine relit. The hardest obstacle... was getting the pilot to try a restart. He just could not believe he shut down the incorrect engine...

"In trainers I can get about 10% of experienced aviators to miss a bright, flashing FIRE light at eye level for up to 5 minutes by introducing multiple emergencies, hurried approaches, and frequent simulated approach-control radio transmissions... The British 737 pilots were in just such a multiple emergency."

Henry Spencer at U of Toronto Zoology  
uunet!attcan!utzoo!henry henry@zoo.toronto.edu

---

## **✶ Hazards of Airliner Computerization**

*Mike Trout <miket@brspyr1.brs.com>*

*Fri, 18 Aug 89 10:42:31 EDT*

Last night on National Public Radio's re-broadcast of BBC news, there was an extensive BBC report on the hazards of airliner crew fatigue. Although the bulk of the report was not earth-shattering and contained nothing particularly new to RISKS readers, there were a few points of interest:

With the increasing computerization of airliner operation, there is less and less for crews to do. Planes are basically flying themselves, and crews have been reduced to monitors. Human beings are notoriously bad monitors; we have a basic desire to "do" things; that is, to solve problems by moving in a step-by-step process, reaching conclusions and beginning work on a new problem. No one is yet suggesting that airliner computerization has gone too far, but all parties admitted that flight crews now routinely fall asleep in the flight deck. This is no longer unusual; studies indicate that sleeping crews are so common that Boeing and other manufacturers are considering adding loud beepers that go off randomly. [Wouldn't it make more sense to give them something constructive to DO?] Many airlines have already adopted official procedures whereby flight attendants are required to visit the flight deck every 15 or 20 minutes to wake up the crew. A former RAF pilot and current editor of \_Flight\_International\_ discussed how in the "old days," it was necessary to flip switches, study analog dials, and mentally compute problems. This kept crews busy on tasks that they knew were critical. Today, all possible factors are displayed on CRT screens, pre-calculated for easy access, whether the crew has asked for the displays or not. This leads to an attitude of complacency and unimportance. Biological time clocks are not well understood, and may play a major factor in crew fatigue. One pilot mentioned that on overwater night flights in which the sun rises in front of the plane, it was virtually impossible to keep awake, even if you weren't tired. The new 747-400, which is flown by only two crew members, always carries a spare crew, as it is designed for extremely long-range flights. Still, no one wants to return to the days of the trans-oceanic flying boats, when journeys took days and everyone, passengers and crew included, was awake during the day and asleep in hotels at night. We pay a price for our "instantaneous" transportation system.

Michael Trout, BRS Information Technologies, 1200 Rt. 7, Latham, N.Y. 12110  
(518) 783-1161

---

## **✶ Re: California studies "drive-by-wire"**

*John Chew <john@trigraph.uucp>*

*Thu, 17 Aug 89 15:11:26 EDT*

In response to Rodney Hoffman <Hoffman.ElSegundo@Xerox.com>'s summary of an article by William Trombley in the Los Angeles Times on 1989 07 24:

Can anyone hypothesize any sort of fail-safe mechanism for the proposed scheme to "platoon" vehicles at 70 mph with 50 foot separation? 50 feet at 70 mph is less than half a second (thank heavens I made it through school before metrification was complete :-)). When the vehicle ahead of you suffers some sort of catastrophic failure of the sort about which RISKS readers lie awake at night contemplating, it seems to me that half a second is insufficient time to reassert manual control, but that any attempt at automatic collision avoidance in a crisis is likely to be a worse alternative. Did the article mention how the system was expected to behave under hazardous circumstances?

john j. chew, iii      phone: +1 416 425 3818    AppleLink: CDA0329  
trigraph, inc., toronto, canada {uunet!utai!utcsri,utgpu,utzoo}!trigraph!john  
dept. of math., u. of toronto    poslfit@{utorgpu.bitnet,gpu.utcs.utoronto.ca}

---

### **✂ First test for electronic tagging starts in jail !**

*Olivier Crepin-Leblond <zdee699@elm.cc.kcl.ac.uk>*  
*Thu, 17 AUG 89 18:51:17 GMT*

Compiled from various short articles in the British Media:

The first person to be electronically tagged has spent the first first night (17 August 1989) of his sentence in prison, since British Telecom has not yet installed a telephone at his house. The man in question is on burglary charges, and is unemployed, and the line will be paid-for by the government. British Telecom has assured that they would complete the installation today, 17 August 89.

This is the first case of electronic tagging, which is on trial here in UK. It has been presented as an alternative for minor jail sentences, to reduce over-crowding of UK's prisons.

Apparently, it is already practised in some states in US. The device is an electronic beeper which is constantly worn by the criminal, and cannot be removed. A central computer makes random telephone calls at the house, where the criminal has to apply the beeper to the receiver, in order to prove that he is present. In this way, the person cannot go more than about 200ft from his phone, and has to stay in his house. There has already been some criticism about this new method, both from the criminal's point of view and the general public. Some say it would be humiliating to wear the tag, since it shows in public. Some say this is the start of "1984" by Orwell, where people's whereabouts are controlled by a computer. Others say that the sentence doesn't have any meaning, since the criminal can enjoy life at home.

The debate is not over, it's only beginning.

disclaimers: all standard ones... tag free.

Olivier Crepin-Leblond  
Electrical & Electronic Eng., Computer Systems & Electronics,  
King's College London, England

**✂ Re: unauthorized Internet activity (CERT Internet Security Advisory)**

<[anonymous]>

Sat, 19-Aug-89 20:52:24 PDT

The original poster suggested using the UNIX utilities "strings", "sum", and "last" to detect a security intrusion. As someone who was once involved from the other side, I would like to suggest that potential victims consider the possibility that these programs have been tampered with. They might be blind to contraband files or other records.

You should also consider the possibility that a contraband file system has been created in the unused disk space of your system.

---

**✂ DEMO Software Disk Infected (Jerusalem Version B)**

SDSV@MELPAR-EMH1.ARMY.MIL <J. Vavrina, Intel & Sec Div, Automation Branch>

Mon, 21 Aug 89 11:34:07 EST

A research and development lab located at Ft. Belvoir Virginia had their PC's infected with the Jerusalem, Version B, Virus. Further investigation uncovered the virus entered the lab through a DEMO software disk from ASYST Software Technologies supplied with a IEEE-488 board from METROBYTE. The infected program is RTDEMO2.EXE.

In a conversation with Mr. Dave Philipson from ASYST, to the best of his knowledge, 50 to 100 copies of the infected software were released. The infection entered their facility through software received from their parent company in England.

Mr. Brent Davis of METROBYTE informed me that the DEMO disk was supplied with three (3) of their products; MBC-488, IE-488 and UCMBC-488. METROBYTE is in the process of contacting all purchasers of these products.

Many thanks to Mr. John McAfee for his assistance, SCAN34 which was used to identify the type of virus, and M-JRUSLM which was used to eradicate the virus.

Both ASYST and METROBYTE were extremely helpful and responded expeditiously to the problem. Many thanks to Mr. Brent Davis and Mr. Dave Philipson for their action and assistance.

Comm 202-355-0010/0011 AV 345-0010-0011 DDN SDSV@MELPAR-EMH1.ARMY.MIL

[This is of course an OLD `virus'. New `viruses' continue to appear. For example, this morning's issue of the VIRUS-L Digest, V2 #178, contains a message from Christoph Fischer <RY15%DKAUNI11.BITNET@IBM1.CC.Lehigh.Edu> (Karlsruhe), entitled NEW VIRUS ['VACSINA'] DISCOVERED AND DISASSEMBLED. For requests to receive VIRUS-L, contact krwv@SEI.CMU.EDU. RISKS long ago stopped trying to include information on virus attacks. 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 9: Issue 15**

**Tuesday 22 August 1989**

## Contents

- [Toronto Stock Exchange down for 3 hours, disk failures](#)  
[Peter Roosen-Runge](#)
- [Automated highways ...](#)  
[Jerry Leichter](#)  
[Bill Gorman](#)  
[Peter Jones](#)  
[Emily H. Lonsford](#)  
[Bill Murray](#)
- [Constructive criticism? Technology doesn't have to be bad](#)  
[Don Norman](#)
- [Computer Ethics](#)  
[Perry Morrison](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **✂ Toronto Stock Exchange shut down for 3 hours by disk failures**

*Peter Roosen-Runge <peter@nexus.yorku.ca>*  
*Tue, 22 Aug 89 11:20:16 EDT*

The following excerpts from Toronto newspapers indicate the reactions expressed following the failure of a Tandem 'non-stop' system at the Toronto Stock Exchange August 16th. Note that the Tandem system did indeed not stop, but the three disc drive failures prevented access to critical market information, without which trading could not continue.

"TSE 'crash' drives trades to Montreal, Brokers curse computer system"  
(Mark Hallman, Financial Post, Thursday August 17, 1989, p. 1.)

A computer crash all but shut down trading on the Toronto Stock Exchange for almost three hours yesterday, forcing tens of millions of dollars' worth of trades to Montreal. ... [the crash] -- a multiple failure within a disc-drive subsystem -- forced a halt at 9:41 AM. ... 'Two pieces of hardware break down and Bay Street breaks down.' said a sour Charles Mitchell, trader. ... 'Who's accountable for that?' ...

A TSE spokeswoman said the failure of both primary and backup systems had never occurred since computers were installed 26 years ago. ...

'Today, the market floors are so automated that when you have this kind of computer failure, there is nothing that can be done', exchange President Pearce Bunting said. 'The greater your dependence on computers, the greater the risks.'

The exchange's computer assisted trading system (CATS) was not affected and smaller stocks continued to trade. But only about 25% of the stocks listed on the TSE are traded using CATS. ...

'Everybody's very much annoyed,' McLean McCarthy's Mitchell said. 'It's costing us a lot of money. I think the people upstairs in the exchange should be held accountable for it.'

[Note: Exchange floor traders failed to haul out the traditional chalkboards to continue trading manually "in the interests of a fair market".]

"Fail-safe Tandem system fails"  
Geoffrey Rowan and Lawrence Surtees  
Globe and Mail, Aug. 17 1989, p. B-1

The stock market crash of 1989 -- yesterday's three-hour trading halt at the Toronto Stock Exchange -- was caused by multiple failures in a computer [Tandem VLX] designed to work even when some of its pieces are broken.

... Peter Richards, president of Tandem Computers Canada of Markham, ont., said the disk drives suffered three separate failures that were a 'once in a lifetime event'. ... Mr. Richards said yesterday's failure was not a computer crash. 'The whole system, minus the data on the one drive, was up and running and available to the exchange during the entire morning. That also meant that recovery was done with the computers on-line, making it a quicker process than with standard computers.'

"TSE seeking to prevent further computer chaos",  
Geoffrey Rowan, Globe & Mail, August 21, 1989, p. B-1, B-4.

... 'Fault-tolerance guarantees that you will not have a problem from any single failure', said John Kane, vice-president for marketing strategy for Tandem. 'I've never heard of three failures at one one time. I don't know what the gods were doing to us.'

[P. H. Roosen-Runge, Dept. of Computer Science, York University, Toronto, Canada]

---

### **Automated highways and the risks of over-sensitivity**

<"Jerry Leichter - LEICHTER-JERRY@CS.YALE.EDU">  
Mon, 21 Aug 89 16:55 EDT

I've been watching the stream of messages deriding as hazardous, impossible,

stupid, etc., etc., the idea of automatic steering of cars on the highway with some bemusement - and concern. The purveyors of the latest bit of technical wizardry are always ready to call it "absolutely safe", "foolproof", and so on. In response, we seem to be developing a "nay-saying" attitude: Any use of computer controls is inherently unreliable, risky, even downright dangerous. This "see no good" response is no better than the "see no evil" attitude of the purveyors!

Let's try to think about the problem of controlling automobiles RATIONALLY for a moment. This is a problem which, WITH SUITABLE DESIGN, is MUCH better solved by machines than by human beings! Driving on a highway consists of long periods of boredom punctuated by random, unpredictable moments in which quick responses are required. People are very bad at dealing with this kind of situation. They get bored, their attention wanders; few are adequately trained to respond quickly, without hesitation or thought, to the near-instantaneous (on the human time scale) dangers which can arise. Computers, on the other hand, cannot get bored, cannot start thinking about their date that evening, and can respond very quickly, without hesitation or panic, if something goes wrong.

It is quite true that a system which mixed human with machine drivers would be very hazardous: Neither is good at dealing with the responses or the abilities of the other. In any case, I'll bet that MOST of the hazards of highway driving are the result of problems with the human drivers, not with the road, the mechanical parts, or other external factors. In some 20 years of driving, I've had my share of scary highway encounters. Without a single exception, they were all clearly the result of poor human decision-making: Unexpected lane changes without checking whether the lane was clear; driving way too fast for the icy conditions of the road and going into a spin at 60 mph; wandering to the edge of the road, touching the curb, then panicking, losing control over the car, and wandering over several lanes of traffic before regaining control. And then of course there are the drunks and the druggies, who account for a large percentage of accidents.

It is also quite true that the highway system as it is designed today was intended mainly for human use. Lane markers that are so clear to the human visual system are notoriously difficult for computers to see, for example. But if the goal is a computerized highway, there is no reason in the world to limit yourself to systems that make sense to humans. A lane marker is hard to track, but a buried wire can be an absolute triviality.

Do you worry about the computers controlling elevators? Elevators have been controlled by digital computers - albeit relay-based - for 30 years or more. They, too, are mechanical devices subject to all sorts of failure.

A computerized driving system, designed for such a purpose, operating in a constrained environment, strikes me as quite practical. It would have to be designed carefully, with "fail-safe" modes - which should be doable since, while tasks like finding the best route to a point 100 miles away require global information and coordination, failing safe requires local information (where are the cars around me, what do their computers claim they intend to do in the next 100 ms., what do my sensors show they actually ARE doing (an essential, and fairly simple backup) and so on.)

Any system can be implemented badly. The structure of some systems makes bad implementations almost inevitable. Computer control of cars on today's road system, in combination with today's drivers, would be such a system - and it seems to be the system most people are commenting on. But it is NOT the system we must necessarily build!

-- Jerry

---

**✂ Re: Drive-by-wire**

*"W. K. (Bill) Gorman" <34AEJ7D@CMUVM.BITNET>  
Mon, 21 Aug 89 16:51:53 EDT*

If one were to compare the potential level of hazard, based, say, on fatalities/100,000 miles, which might arise from failure of on-board computers as opposed to the current levels of fatality caused by intoxicated and/or drugged-out drivers, heart attacks, strokes, vehicular suicides, driver error, police chases, etc., I wonder which methodology (hardware vs. wetware) would actually be safer, once all the emotional rubbish about "men vs. machines" was cleared away? Just a thought...

---

**✂ California studies "drive-by-wire" ([RISKS-9.14](#))**

*514)-987-3542 <Peter Jones <MAINT@UQAM.bitnet> (>  
Mon, 21 Aug 89 16:27:10 EDT*

Bring back the trains, buses and streetcars. These are well-proven, reliable, non-polluting ways of moving large numbers of people from place to place. My intuition is that the problem of controlling thousands of automobiles from a central point would rival Star Wars in complexity.

---

**✂ Re: Automatic vehicle systems ([RISKS-9.14](#))**

*Emily H. Lonsford <m19940@mwvm.mitre.org>  
Monday, 21 Aug 1989 18:04:55 EST*

Don't worry too much about these. If we can't get people to ride public transportation (like buses and subways) then they won't sit still for the equivalent in their own cars. And anyway, how do you get off the "remoteway" to stop at the cleaners?

Emily H. Lonsford, MITRE - Houston W123 (713) 333-0922

---

**✂ Automated Highways**

*<WHMurray.Catwalk@DOCKMASTER.NCSC.MIL>  
Mon, 21 Aug 89 19:37 EDT*

>Call me a technophobe if you like, but \*NOBODY\* can guarantee 100% ...

Well, it must be nice to live in the UK. Here in the US we have a very reliable manual system. It can be so relied upon to kill 40,000 people a year that we simply take it for granted. A large percentage of these deaths involve malicious manipulation of the system, i.e., the ingestion of alcohol and other drugs. You may be able to tolerate these deaths in preference to the risk of computer systems that are less than perfect. Quite candidly, I am sick to death of a system that tolerates and defends this carnage, while crying crocodile tears about computer-related risks. It is high time that we got a system for comparing risks that is prepared to put these lives on the same scale that we use to condemn research into alternatives.

The New York Times concluded in a front page article that the American people are far more likely to tolerate the huge death toll from their discretionary and recreational use of highways, tobacco and alcohol than risks which are comparatively minuscule from automated systems. I may be stuck with that, but it is insane and elitist. It is high time somebody said so.

William Hugh Murray, Fellow, Information System Security, Ernst & Young  
2000 National City Center Cleveland, Ohio 44114  
21 Locust Avenue, Suite 2D, New Canaan, Connecticut 06840

---

### **✂ Constructive criticism? Technology doesn't have to be bad**

*Donald A Norman-UCSD Cog Sci Dept <[norman%20cogsci@ucsd.edu](mailto:norman%20cogsci@ucsd.edu)>  
Tue, 22 Aug 89 09:09:38 PDT*

This has been brewing for a long time. I enjoy the RISKS forum and tout RISKS as the best digest available on e-mail/netnews. But sometimes I wonder. Submitters seem to take great glee in presenting YAHS (Yet another horrible story), but I seldom see any constructive comments -- or much discussion at all -- mostly it is simply story time. And most of the stories are about why we should not trust technology. But the unaided human is even less reliable than the aided one! Surely we could use the stories as design examples and attempt to use them to inform our design, so that we could invent technologies that were real improvements. Instead of using the examples for a cheap laugh, how about using them for instruction?

Let me provide some examples, using [RISKS DIGEST 9.14](#) as my example, both because it is handy and also because it had an excess of scare stories and cheap conclusions.

- - -

1. Misdelaivered mail because the barcode had the wrong zipcode, and the machines read it and ignored the written address. Moral: I would say that you should not use code that was only machine readable. Either do like the banks do -- invent a machine-readable text that humans can also read -- or do as supermarkets do - print the "English" version of the bar code beneath the bar code. This would make it a lot easier to catch errors of this sort. (The best solution is to make postal machines that can read the handwriting on the envelopes, but that is another decade away, at least). (Because barcode is already standardized as the postoffice system, why not require English text to be printed beneath the barcode? No change in equipment is required at the Post Office end.)

- - -

2. Automatic vehicle navigation systems. RISK readers are really scared of this one, to judge by the number of times this is raised in RISKS. But what are the alternatives? Today we have roughly 50,000 fatalities a year in the auto. If driving were all done automatically, there would be occasional massive screwups. But would the death toll hit 50,000? I bet it would improve things. (Yes, roughly 1/2 of those deaths have drinking implicated, but I don't see how this changes my argument.) These systems in aviation are reasonably efficient.

Moreover, I see no reason why we couldn't make these things fail reasonable softly, with lots of warning. And yes, there would still be foul-ups, but the baseline is not zero accidents -- it is 50,000 deaths). (Admission of guilt: I am consulting for a company that is designing one of these automated systems.)

- - -

3. One submitter's statement that "I am amazed that Boeing has taken all the blame... " for pilot's shutting down the wrong engine. The submitter than cites other examples of pilots shutting down wrong engines, implying that this is clearly pilot error (since it happens often and in various aircraft). So Boeing -- or any particular manufacturer is clearly not at fault. I disagree.

This error has long been noted, first well documented in the 1940's. But it is the design of the cockpit controls that leads to the error. So I would still blame Boeing (or cockpit designers in general). I have long thought that many control panels are designed as if to increase the chance of error (my experience is mostly in nuclear power and aviation), and that there are redesigns -- perhaps using better technology -- that would minimize these errors. Shutting off the wrong engine is so common (relatively speaking), that more design effort should have gone into finding better systems. Instead, folks just blame the pilot. That is the wrong attitude.

Look, people make errors. Fact of life. Therefore, good design will anticipate those errors and make them either impossible or less likely, or easier to detect and correct.

(Admission: I am off to Boeing next week to discuss cockpit design. This note will not win me friends at Boeing.)

- - -

4. The report of airliner crew fatigue. Cockpit crew fall asleep and so cabin crew are now supposed to wake them up, or there are systems that blast them with loud sounds.

My solution is quite different: let them sleep!

It is well known that the circadian rhythm has two minima -- about 2PM and 2AM. And flying long hours across time zones is hard on the system. Suppose you let crew take naps. As long as at least one member stayed awake, and if the nap were announced and known about, there is likely to be no problem. Modern aircraft can be flown with one crew member: more are needed only in emergencies and in periods of high workloads (e.g., takeoff and landing or in crowded airspace at low altitudes). In fact, some airlines are experimenting with allowing short naps. The point is, human biology should be lived with,



Cautionary Tales and Ethical Dilemmas in Computing  
by Tom Forester and Perry Morrison

Published by MIT Press and Basil Blackwell  
To Appear (Hopefully) January 1990

CONTENTS

Preface and Acknowledgments

1. Introduction: Our Computerized Society

Some Problems Created for Society by Computers - Ethical Dilemmas for Computer Professionals and Users

2. Computer Crime

The Rise of the High-Tech Heist - Is Reported Crime the Tip of an Iceberg? - Targets of the Computer Criminal - Who Are the Computer Criminals? - Improving Computer Security - Suggestions for Further Discussion

3. Software Theft

The Growth of Software Piracy - Revenge of the Nerds? Intellectual Property Rights and the Law - Software Piracy v. Industry Progress - Busting the Pirates - Suggestions for Further Discussion

4. Hacking and Viruses

What is Hacking? - Why Do Hackers 'Hack'? - Hackers: Criminals or Modern-Day Robin Hoods? - Some "Great" Hacks - Worms, Trojan Horses and Time-Bombs - The Virus Invasion - Ethical Issues - Suggestions for Further Discussion

5. Unreliable Computers

Most Information Systems are Failures - Some Great Software Disasters - Warranties and Disclaimers - Why are Complex Systems So Unreliable? - What are Computer Scientists Doing About It? - Suggestions for Further Discussion

6. The Invasion of Privacy

Database Disasters - Privacy Legislation - Big Brother is Watching You - The Surveillance Society - Just When You Thought No One was Listening - Computers and Elections - Suggestions for Further Discussion

7. AI and Expert Systems

What is AI? - What is Intelligence? - Expert Systems - Legal Problems - Newer Developments - Ethical Issues: is AI a Proper Goal? - Conclusion: the Limits of Hype - Suggestions for Further Discussion

8. Computerizing the Workplace

Computers and Employment - Computers and the Quality of Worklife: 'De-skilling' - Productivity and People: Stress, Monitoring, Depersonalization, Fatigue and Boredom - Health and Safety Issues: VDTs and the RSI Debate - Suggestions for Further Discussion

APPENDIX A Autonomous Systems: the Case of "Star Wars"

Preface and Acknowledgements

The aim of this book is two-fold: (1) to describe some of the problems created for society by computers and (2) to show how these problems present ethical dilemmas for computer professionals and computer users.

The problems created by computers arise, in turn, from two main sources: from hardware and software malfunctions and from misuse by human beings. We argue that computer systems by their very nature are insecure, unreliable and unpredictable - and that society has yet to come to terms with the consequences. We also seek to show how society has become newly vulnerable to human misuse of computers in the form of computer crime, software theft, hacking, the creation of viruses, invasions of privacy, and so on.

Computer Ethics has evolved from our previous writings and in particular our experiences teaching two courses on the human and social context of computing to computer science students at Griffith University. One lesson we quickly learned was that computer science students cannot be assumed to possess a social conscience or indeed have much awareness of social trends and global issues. Accordingly, these courses have been reshaped in order to relate more closely to students' career goals, by focussing on the ethical dilemmas they will face in their everyday lives as computer professionals.

Many college and university computer science courses are now including - or would like to include - an ethics component, but this noble objective has been hampered by a lack of suitable teaching materials. Computer Ethics has therefore been designed with teaching purposes in mind in an effort to help rectify the shortage of texts. That is why we have included numerous up-to-date references, as well as scenarios, role-playing exercises and 'hypotheticals' in the 'Suggestions for Further Discussion' at the end of each chapter. The creative teacher should be able to build on these.

Readers will notice that we have not adopted an explicit theoretical framework and have avoided philosophical discussion of ethical theory. The reason is that this book is but a first step, with the simple aim of sensitizing undergraduate computer science students to ethical issues. Neither will readers find a detailed account of the legislative position around the world on the various topics discussed. This is because in each country the legal situation is often complex, confused and changing fast - and again this is not the purpose of the book.

Finally, a note on sources. First, we have to acknowledge an enormous debt to Peter G. Neumann, whose "Risks to the Public in Computer Systems" sections in Software Engineering Notes, the journal of the Association of Computing Machinery's Special Interest Group on Software (ACM-SIGSOFT) have provided inspiration, amusement and a vast amount of valuable information. Long may he continue. Second, we have to caution that many of these and other sources are newspaper and media reports, which, like computers, are not 100 per cent reliable.

Tom Forester, School of Computing & Information Technology Griffith University, Queensland, Australia	Perry Morrison Maths, Stats and Computing University of New England Armidale, NSW, Australia
--	---



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

**Volume 9: Issue 16**

**Wednesday 23 August 1989**

## Contents

- [Autopilots](#)  
[Marc Rotenberg](#)
- [Hazards of Airliner Computerization](#)  
[Brinton Cooper](#)
- [Risks, and an assumed definition of "reliability"](#)  
[Bob Estell](#)
- [Computers in Medicine](#)  
[Brinton Cooper](#)
- [Constructive criticism? Technology doesn't have to be bad](#)  
[Donald A Norman](#)
- [Tandem computers and stock exchange failure](#)  
[Ernest H. Robl](#)
- [TSE shutdown -- a success story](#)  
[Rich D'Ippolito](#)
- [Incompatible IR controllers damage circuits?](#)  
[David A Willcox](#)
- [Re: a balancing act for wheel watchers](#)  
[J. Eric Townsend](#)  
[Keith D Gregory](#)
- [Info on RISKS \(comp.risks\)](#)

---

### Autopilots

<[mrotenberg@cdp.uucp](mailto:mrotenberg@cdp.uucp)>

Tue, 22 Aug 89 16:53:25 -0700

The New York Times, August 12, 1989

Automated Planes Raising Concerns, by Carl Levin

Airlines are starting to fly a new generation of highly automated jets, raising concerns among safety researchers that pilots will rely too much on the technology and will lose or never learn the sharp skills and reflexes needed in emergencies.

The first scientific study to compare pilots' performance in highly automated and traditional cockpits began Tuesday in Atlanta. Researchers at the Federal Aviation Administration and the National Aeronautics and Space Administration said the results would help them improve training for pilots who fly the advanced planes and suggest ways to better design future craft.

The most advanced planes, like the Airbus A320 and Boeing's 757 and 767 models, require little of the hands-on flying skill that older models need. For years, planes have had autopilots to keep level and make simple turns, but with the newest equipment pilots can push a few buttons and lean back while the plane flies to its destination and lands on a predetermined runway. Virtually every calculation is made by computer.

#### More Control to Machines

"We're taking more and more of those functions out of human control and giving them to the machines," said Dr. Clay Foushee, the chief F.A.A. scientist for human performance issues. "The question becomes whether humans will really respond when something goes wrong."

Aviation experts cite the performance of the pilots of two disabled United Airlines jets in recent months as examples of how basic flying skills and years of experience can make a big difference in emergencies.

After a disintegrating tail engine crippled the hydraulic system on a DC-10 on July 19, Capt. Altred C. Haynes, a 33-year United veteran, and his crew devised a way to crash-land the plane in Sioux City, Iowa. Of the 296 people aboard, 185 survived.

Capt. David M. Cronin, also a United pilot for three decades, cited his crew's extensive experience in the safe landing of his Boeing 747 in Honolulu in February after a cargo door and large section of fuselage blew off the plane, knocking out two of its four engines and killing nine passengers:

#### Airlines See New Planes as Safer

"Here's two examples of unforeseen Qand in fact some engineers would have said impossible Qtypes of failures that were dealt with creatively by human operators," said Bob Buley, a flight standards manager at Northwest Airlines. "If we have human operators subordinated to technology then we're going to lose that creativity. I don't have computers that will do that; I just don't."

Airlines like the equipment because it keeps a plane closer to its course than a pilot can, cutting costs and increasing safety in some operations.

The head of pilot training for United William H. Traub, said that the carrier had been flying highly automated Boeing 767's since 1982 and that he knew of no deviations greater than 300 feet from assigned altitudes. "In that respect it's a safer system," he said in a telephone interview.

Leading the parade of new technology is the A320, a jetliner made by the European consortium Airbus Industrie, which began passenger service in this country last month. Northwest is buying 100 of the jets and has started flying

the first two. Braniff, with 50 on order and 50 on option, plans to put its first A320 into service this month.

In addition to the increased use of automatic cockpit controls, the A320 eliminates virtually all direct mechanical or hydraulic links to movable surfaces on the wings and tail that direct a plane's speed and angle of flight. Five computers translate a pilot's actions into electronic commands that move surfaces, changing the plane's speed and direction.

Computers can control the speed and direction of flight more accurately than any human pilot but even aviators who defend the A320 say the extensive use of automation raises questions about a pilot's ability to respond quickly in an emergency.

Looking for 'Ideal Balance'

"In my perfect world we marry the advantages of automation and the creative attributes of human operators," said Mr. Buley of Northwest. "The A320 is a quantum leap ahead. What I'm looking for is the ideal balance, and I'm not sure we've reached that with that airplane."

The equipment on the new planes is more reliable than before, and it can relieve pilots of routine duties that might distract them from more important tasks. For example, in the Boeing 767, computers automatically calculate and adjust the descent speed to use the least fuel for the distance traveled, one pilot noted. In the older Boeing 727, pilots go through "constant mental gymnastics" to make the calculation themselves, the pilot said.

But just as some educators argue that a pupil with a calculator might not learn basic principles of mathematics, aviation researchers say pilots who depend too much on computers might not be as quick to determine the correct descent speed on his own if the computer fails as would the 727 pilot who does this on every flight.

Cockpit crew complacency and boredom are another issue, and these problems are highlighted by a separate airline industry study of automation and pilot performance. The F.A.A. and the National Aeronautics and Space Administration are building on the airline study and the Atlanta research to develop a national program to improve the ways technology is used in aviation.

Other concerns listed by the airline group, led by Mr. Buley of Northwest, include the problems pilots face when automated equipment fails and the deterioration of basic flying skills.

Pilots Share Concern

Pilots themselves share these concerns, according to a recent space agency study of 200 pilots who have been flying the Boeing 757 for airlines. About half agreed with the statement "I am concerned about a possible loss of my flying skills with too much automation." Even so, nearly 90 percent of the pilots agreed that the new instruments were "a big step forward."

Many of these questions will come up again Sept. 18-19 when Dr. Foushee and

representatives from manufacturers and airlines meet to discuss the national plan for improving the way people use technology in aviation.

Adding to the urgency of the research is the current boom in pilot hiring. Over the next decade a new generation of pilots will be climbing into cockpits, and virtually all their airline training will come in the new jets.

"What happens when the automation fails?" asked Earl L. Wiener of the University of Miami, an expert in pilot performance who is directing the Atlanta study. "A collision is coming between very inexperienced pilots and very sophisticated aircraft."

To be sure, today's pilots have the advantage of extensive training on advanced cockpit simulators, which duplicate every movement a plane would make. A pilot in a simulator can practice flying after losing various computer and control systems.

"There have been many simulator advances that hopefully will give pilots training advantages that an older generation of pilots didn't have," Dr. Foushee said.

Still, while simulator training could help for some kinds of emergencies, others, like the loss of the hydraulic system in the DC-10 in Iowa, are considered so remote that pilots do not train for them on simulators.

Besides examining how well pilots respond in emergencies, researchers hope to examine any differences in the ways pilots work with one another in automated and conventional cockpits, said Dr. Everett Palmer of NASA's Ames Research Center, which is financing the study led by Dr. Wiener.

---

## **✦ Hazards of Airliner Computerization**

*Brinton Cooper <abc@BRL.MIL>*

*Tue, 22 Aug 89 17:04:57 EDT*

Mike Trout quotes BBC News, ... pointing out that flight crews need to do something "critical" to the success of the flight. The solution may be right under our noses.

How often, in this forum, have we discussed applying tests of "reasonableness" to computer-generated answers to problems? It seems that such tests are critically needed in the cockpit, the most obvious example being Flight KAL 007. Such reasonableness checks as humans would be capable of performing, would be far from "make work" and would reduce significantly some of the risks associated with increasingly automated flying.

...or so it seems from here.

\_Brint

---

## **✦ Risks, and an assumed definition of "reliability"**

"FIDLER::ESTELL3" <estell3%fidler.decnet@nwc.navy.mil>

22 Aug 89 15:51:00 PDT

[RISKS 9.15](#) highlighted a phenomenon [I am tempted to say, "problem."] that I've noted in RISKS for some time:

We tend to want computerized systems to be very much more reliable than non-computerized systems.

For example, is my Seiko watch reliable? Yes. Has it ever failed?

Yes; the original battery ran down after 5 years. Does it run exactly in synchronization with the Naval Observatory master clock?

No; it gains about a second a week. Is that OK? Yes! It's great!

Is my old '66 Pontiac reliable? Yes. Has it ever failed? Sure; batteries have gone dead; a tire blew out; water pump failed (at about 90K miles); alternator failed (about the same time); tune ups needed every 3 years; ... I've probably belabored the point too long already.

Folks, we've been spoiled by our own successes. I'm all upset with the maker of the hard disk in my Mac II, because it needs to be replaced after only 18 months. I have to stop and think about where I began, in 1960. The computer we had then was less than 10% the horsepower of my Mac; it had a miserable collection of "user tools" - the best being a FORTRAN II (yes, "2") compiler. And it went down at least 4 hours every week for "maintenance." And it cost a million dollars (or so); so the whole base [not China Lake] got by on just one.

But can we improve? You bet. My Norelco shaver [first one] lasted 7 years; that's a lot better than the hard drive in either my old Mac +, or this Mac II. Maybe Norelco should teach "brand X" disk drive maker about motors?

Bob

---

## **✂ Computers in Medicine**

Brinton Cooper <abc@BRL.MIL>

Tue, 22 Aug 89 23:56:50 EDT

We seem to have more than our share, in the Digest, of horror stories about computer failures in stock exchanges, motor vehicle records, aircraft control systems, weapons control systems, and banking applications. While I have not sampled the subjects scientifically, it seems as if we've not had quite so many horror stories in medical applications. (Of course, I'm not asserting that there have been none!)

Several years ago, a few colleagues from the Lab and myself consulted with the Shock-Trauma Unit of the Maryland Institute for Emergency Medical Service Systems regarding their use of computing in clinical applications. At the time, they used a DEC computer for patient records, testing results, pharmacy and medical orders, etc. It included software which "integrated" these applications so that the attending physician could trace the effectiveness of medicines and therapies with time. (Shock-Trauma gets the most seriously injured patients, often flown in by the MD State Police in helicopters landed on premises.)

An important concern of the medical personnel at the time was computer failure. Although the physicians initially resisted the machines' intrusion into their domain, they had ultimately been "won over" and became quite fond of and dependent upon the computer. Virtually every medical person in the unit learned, voluntarily, how to re-boot the system in the event of a crash -- which was relatively often. This was the late 1970s. They wanted to know if they could justify the funds to purchase a fully redundant system. There were two interchangeable computers doing different functions (one was not critical). They felt that a third machine would give them the security of always having their data available, but they needed justification and support from so-called "experts," i.e. us.

Well, we gave them what they needed, but that is not the point of the story. The points are:

1. Is my perception correct? Are there proportionally more life and property threatening computer-related faults in banking, transportation, and national defense than in medical applications?
2. If there's even a modicum of truth in #1, then why? Certainly the hardware and software aren't unique in the hospital. Is it a matter of how they're used? Is there more emphasis on redundancy and reliability and less on moving it faster and making another buck? Are the machines introduced into new applications more gradually, so that users are assured of correct operation at every step of the way?
3. Or are the physicians merely burying their mistakes again?

\_Brint

---

### **✂ Constructive criticism? Technology doesn't have to be bad**

*Donald A Norman-UCSD Cog Sci Dept <norman%[cogsci@ucsd.edu](mailto:cogsci@ucsd.edu)>  
Wed, 23 Aug 89 09:47:53 PDT*

I like the Petroski book ["To Engineer is Human: The Role of Failure in Successful Design"]. It is an excellent example of design and the problems that are inherent in pushing technology beyond what science can yet (ever?) provide.

This is especially true when people chide me about human interface technology and say something like "How come interface design isn't `scientific', like, say, bridge design." I tell them to read Petroski and then tell me about bridges.

I recommend Petroski to all my friends and students. (I am happy to say that someone told me that he, in turn, recommended my book.)

don

---

## **✂ Tandem computers and stock exchange failure**

*Ernest H. Robl <ehr@uncecs.edu>*

*Wed, 23 Aug 89 11:49:57 EDT*

The quoted reports on the problems with the Tandem system at the Toronto Stock Exchange are a good example of the difficulty the news media have with reporting on complex technological stories.

As someone who works with a Tandem system, I can point out a few things that may be of value to Risks readers:

Tandem computers do not have "backup systems" as such. Instead, the design incorporates redundant components -- all of which perform work under normal conditions. The minimum system Tandem will normally sell you is one with TWO CPUs, and at least one of the discs (\$System -- the one with the operating system) mirrored.

How failsafe a system is depends a lot on how the system is configured. Most Tandem systems have at least some of the discs unmirrored. (That's usually an economic decision.)

With mirrored discs, data is always written to both discs. However since it needs to be read from only one, there are situations where different reads can be performed at the same time on the two halves of the mirrored pair -- which will actually provide a gain in performance for some operations.

Based on the quoted reports, I assume that the failures at the stock exchange involved both halves of a mirrored disc pair -- though that's not obvious. I'd be interested in hearing additional details, if they are reported. (Mail to me, if you don't think this is of interest to the Risks audience.)

My opinions are my own and probably not IBM-compatible.--ehr  
Ernest H. Robl (ehr@ecsvax) (919) 684-6269 w; (919) 286-3845 h  
Systems Specialist (Tandem System Manager), Library Systems,  
027 Perkins Library, Duke University, Durham, NC 27706 U.S.A.

---

## **✂ TSE shutdown -- a success story**

*<rsd@SEI.CMU.EDU>*

*Wed, 23 Aug 89 12:38:08 EDT*

In [RISKS 9.15](#), Peter Roosen-Runge brings us the following quotes:

A computer crash all but shut down trading on the Toronto Stock Exchange for almost three hours yesterday, forcing tens of millions of dollars' worth of trades to Montreal. ... [the crash] -- a multiple failure within a disc-drive subsystem -- forced a halt at 9:41 AM. ... 'Two pieces of hardware break down and Bay Street breaks down.' said a sour Charles Mitchell, trader. ... 'Who's accountable for that?' ...

A TSE spokeswoman said the failure of both primary and backup systems had never occurred since computers were installed 26 years ago. ...

My rough calculations indicate that the system availability has been 99.9986% for those 26 years. Who, indeed, IS responsible for that -- give them a reward!

'Everybody's very much annoyed,' McLean McCarthy's Mitchell said. 'It's costing us a lot of money. I think the people upstairs in the exchange should be held accountable for it.'

How much were these people making with the chalkboard system?

It is human nature to demand perfection from everyone and everything else. Have these folks ever heard of business insurance? It should have been very inexpensive given the prior availability of the system.

Along with our efforts to reduce risks in our trade, do we not need to educate users in risk management?

Rich D'Ippolito

---

### **✂ Incompatible IR controllers damage circuits?**

*David A Willcox <willcox@urbana.mcd.mot.com>  
Wed, 23 Aug 89 09:36:15 -0500*

I few weeks ago, I spent a couple of nights at a fairly nice hotel on the East Coast. You could tell it was a nice place because the remote control for the TV was not bolted to a table.

I was intrigued by the notice that was pasted to the remote:

CAUTION: The frequency of this television remote will damage the internal electronics of any set not programmed to receive the spectradyne signal.

My first reaction was to chuckle at this rather obvious attempt to scare light-fingered but gullible clientele out of "offing" the remote. But I got to wondering. Is there any possible truth to this? If there is, how do I know that my VCR remote, say, won't damage my TV? And if my TV was damaged, wouldn't that be evidence of really poor design?

I suspect that the worst "risk" here is that some guests of this hotel are going to get a very warped idea of reality.

---

### **✂ Re: (a balancing act for wheel watchers)**

*J. Eric Townsend <erict@flatline.sbc.com>*

21 Aug 89 17:49:14 CDT (Mon)

Actually, many computerized balancing/alignment systems are very, very simple (even for mechanics :-). Monitoring devices are attached to the wheels while the car is on a lift. The car's data is looked up in a book and entered in by hand on a large number of the machines. (I have a car not in "the book" and have had to provide my own data.) Then you procede to align/balance by looking at a rather basic "under/correct/over" meter for each wheel.

There are probably a half-dozen other ways to do balancing/alignment, and probably a thousand variations on the above theme...

J. Eric Townsend, 511 Parker #2, Houston, Tx 77007

---

**✂ Re: Tired of computers being trusted? (a balancing act for wheel watchers)**

Keith D Gregory <keith@fstohp.lynn.ge.com>

Tue, 22 Aug 89 09:19:54 edt

More likely, the mechanic was not "machine literate". I ran into a similar problem: I had a flat repaired, and the shop (run by the company that made the tires) balanced the tire as part of the repair. At the same time, I purchased a "lifetime balancing and flat repair" contract. Driving home, I noticed a slight shimmy that wasn't there that morning. The next morning, I took the car in for a complete rebalancing.

And when I drove home, the shimmy was worse - much worse. The next day, I went back to the shop and complained. This time I watched as the tires were balanced. What had happened was that the "mechanic" (I use that term loosely) did not have a properly sized chuck for the wheel balancing machine. So he used one that was "close". As a result, the wheel was able to move from side to side while it was being tested, with the result that the weights were put in random (?) locations.

The moral? If you don't trust computers, don't trust the people that do.

-kdg

[So it would be very easy to key in wrong data for the given car, or correct data for the wrong car, etc. Thanks. 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 9: Issue 17

Wednesday 23 August 1989

## Contents

- [Hazards in Airlines and Medicine](#)  
[Nancy Leveson](#)
- [Re: Technology Doesn't Have to Be Bad](#)  
[Mike Trout](#)  
[Robert Dorsett](#)
- ["Drive-by-wire": What about bicycles?](#)  
[Anne Paulson](#)  
[Donald A Norman](#)
- [Re: Autopilots](#)  
[Brinton Cooper](#)
- [Re: Automated Highways](#)  
[George H. Feil](#)
- [Roads made safer or not?](#)  
[Pete Lucas](#)
- [Training & Software Engineering, a reply...](#)  
[Edward A. Ranzenbach](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✉ Hazards in Airlines and Medicine (Brint Cooper, [RISKS-9.16](#))

Nancy Leveson <[nancy@murphy.ICS.UCI.EDU](mailto:nancy@murphy.ICS.UCI.EDU)>

Wed, 23 Aug 89 11:45:03 -0700

Subject: Hazards of Airliner Computerization (Brint Cooper, [RISKS-9.16](#))

>Such reasonableness checks as humans would be capable of performing,  
>>would be far from "make work" and would reduce significantly some of the  
>risks associated with increasingly automated flying.

Such reasonableness tests in software are not easily constructed. It is much more difficult to do than you seem to think.

Subject: Computers in Medicine (Brint Cooper, [RISKS-9.16](#))

> 1. Is my perception correct? Are there proportionally more  
> life and property threatening computer-related faults in banking,

> transportation, and national defense than in medical applications?

No. No, there are not. There are proportionally the same given the relative complexity of the systems and the amount of use.

> 2. If there's even a modicum of truth in #1, then why?

There is no truth in it.

> 3. Or are the physicians merely burying their mistakes again?

Be careful to have your facts before attacking a group of people. In fact, medical computer problems are more carefully reported because the FDA requires this while there are not similar requirements in other applications. There are large numbers of reported computer errors and recalls in the FDA database.

I have noticed, however, that many medical equipment manufacturers take quality control more seriously than some other industries because of the potential liabilities and costs involved in an FDA-ordered recall of a medical device.

---

### **🔥 Re: Technology Doesn't Have to Be Bad ([RISKS-9.15](#))**

*Mike Trout <miket@brspsy1.brs.com>  
23 Aug 89 17:06:15 GMT*

Don Norman (dnorman@ucsd.edu) writes:

> 4. The report of airliner crew fatigue...

My profound apologies for omitting part of the BBC report; I typed it in from memory. Don's statements reminded me that the BBC report included considerable discussion on the subject of allowing aircrew napping. The basic argument was generally that which Don raised, i.e., that minor aircrew napping would actually make things safer. It did, however, sound like the "powers that be" were rather reluctant to allow the public to know that the folks up front may be sawing logs.

As an aside, a few weeks back NPR had an extensive report on napping. The contention was that studies conclusively show that napping dramatically improves concentration, productivity, and the ability to deal with problems. Yet society strongly disapproves of napping, and anybody caught napping on the job will be very lucky if they don't get fired. Napping is viewed as "wasted time"; time which could be spent doing something "constructive." Never mind that major portions of most workers' afternoons are often spent in an advanced state of bleary-eyed semi-coherence. It will be a long time before this attitude changes, despite the fact that some of history's most effective personalities, such as Winston Churchill, took frequent naps.

Michael Trout, BRS Information Technologies, 1200 Rt. 7, Latham, N.Y. 12110  
(518) 783-1161

## **✂ Re: Technology Doesn't Have to Be Bad ([RISKS-9.15](#))**

Robert Dorsett <mentat@walt.cc.utexas.edu>

22 Aug 89 23:52:50 GMT

Don Norman wrote:

>... It is well known that the circadian rhythm has two minima -- ...

1. It's extremely difficult to apply simple principles of the analysis of circadian rhythm when the crew in question might be transiting multiple time-zones, on a continuous basis, on irregular schedules.
2. Part of the problem is cockpits that lull their pilots to sleep. In *The Journal of Navigation*, an oft-repeated statistic through 1983 and 1984 was that Britannia Airways found that 767 cockpit crews were far more sedate (lower heart rates) than those flying the 737. This was ascribed to better-designed seating, noise reduction, and low workload.

In cruise, modern crews are given very little to do. To address this problem, very positive steps are being taken--such as having the stewardess check in, airline policy requiring manual calculation of navigation problems, mandatory (unnecessary) radio call-ins every fifteen minutes, etc. I see no reason to criticise such measures: they attempt to make the best of what is becoming increasingly clear is a bad situation.

3. Operational practice on many airlines (even if it's not *\*policy\**) IS to let a pilot take a snooze if he just can't keep his eyes open. The other pilot's notified, and the guy takes a nap. Great. But that reduces the redundancy in a modern cockpit by half. So what happens if the remaining guy (often on the same sleep-schedule) falls himself nodding off? (if you've never flown long-distance, it's quite startling, after being *\*awake\** 25 hours or so, to suddenly wake up--without ever discovering you had fallen asleep). Modern autopilots are incredibly reliable, and it's easy to argue that there's nothing wrong with even *\*both\** pilots napping for a while. The problem is that, even in cruise, even with modern flight assist mechanisms, problems can manifest themselves faster than the crew can "get back into the loop." One of the recommendations of the NTSB report on the China Airlines flipover over Los Angeles a few years ago was to bring pilots closer into the control loop.

My personal gripes with flight automation are:

- \* Lack of experience. Automation's a new concept. We have little experience dealing with the human factor in automation design.
- \* Economics-oriented vs. safety-oriented design. It's always possible to fund a study that supports the manufacturer's viewpoints. Even if backhanded techniques aren't used, genuine divisions exist within the industry on the place and role of automation.
- \* Lack of human-factors influence in system design (letting the engineers have at it).
- \* Too much human-factors influence in system design (psychologists pushing

pet theories in safety-critical situations).

(the above really boils down to lack of \*operations\* influence in system design, but even that's not always a help--consider a system designed to pilot specifications, which leaves the pilots with precious little to do).

\* Relatively low lack of computer literacy among pilots (the more microprocessors the better), and consequent over-reliability on automation (Cf. my article in [RISKS 9.13](#)).

\* Unfounded fault-probability claims by manufacturer (both in program verification and hardware reliability).

\* Lack of standardization. How one airplane does something is not necessarily how another one does it (look at airspeed displays on the 747-400, Fokker 100, A320, and A310). Not even COLORS are standardized.

In my opinion, not nearly enough muckraking is being done on the risks of automation in aviation (and other disciplines). When computers are marketed on the mere basis that they're high-tech, and purchased, respected, and put in safety-critical situations solely on that basis, it's time to worry. I think RISKS serves a purpose by bringing such problems to our attention. And I, for one, do not "get a laugh" out of reading about how yet another implementation has been botched up.

---

### ✂ "Drive-by-wire": What about bicycles?

Anne Paulson <PAULSON@INTELLICORP.COM>  
Wed 23 Aug 89 12:31:23-PST

Another opinion on "drive-by-wire" systems:

I, like many other submitters, am against them, but for a reason not yet brought up. Designers of automated traffic-control systems have an unfortunate tendency to design for cars, and forget about other road users, like cyclists and pedestrians.

A case in point is the "smart" traffic light, which is actuated by automotive traffic. There are a lot of these menaces where I live. They work fine for cars, sure. But try to make a left turn when you're riding a bike. You get in the left-turning lane, right on top of the sensor, in hopes that it will notice you. If you are riding a steel bike, you have about a 70% chance that the light will turn for you. The sensors, I believe, work by magnetic inductance, so if you're riding an aluminum bike (as I do) you have a less than 50% chance that the light will turn for you. Of course, if the light doesn't turn, you are forced to run it. This is more dangerous than if there were no light there, because the drivers going straight through think they have the right of way, and aren't expecting turning traffic. Another problem for cyclists is that "smart" lights often go green for only an instant, so that if the road is crowned, it's difficult to get through the intersection while the light is still green (or, in some egregious cases, while it's still yellow).

These smart lights often endanger pedestrians, too. A block and a half from my office is a "smart" T intersection. For a long time, the light was adjusted so that left-turning traffic and pedestrians would be in the same place at the same time. (I think the designers forgot that this was a T intersection, so that all the traffic would be turning left.) Again, it was particularly dangerous because the drivers thought that the pedestrians were jaywalking, when in fact the pedestrians had a green light. Finally, after at least three years, the problem was "fixed" by barring pedestrians from crossing there at all.

Technology lovers might argue that these are design flaws that could be fixed. This is true, but they haven't been. (I, and other members of my bicycle club, routinely call the cities and counties when we find lights that don't turn for us, but we rarely get satisfaction. And why should it be up to us to make sure the lights work, anyway?) I don't believe that "drive-by-wire" systems would be any better.

By the way, where I live, the number of cyclists is not insignificant. In Santa Clara County, twice as many people commute by bicycle as commute by mass transit.

I would be happy to hear from Donald Norman, or other people working or consulting for companies that are designing "drive-by-wire" systems, on how such systems will allow for cyclists.

-- Anne Paulson, Intellicorp, 1975 El Camino Real, Mountain View, CA

---

### ✂ "Drive-by-wire": What about bicycles?

*Donald A Norman-UCSD Cog Sci Dept <norman%cogsci@ucsd.edu>*

*Wed, 23 Aug 89 14:34:51 PDT*

My long diatribe in RISKS has generated the proper result: numerous people have written me and several, as this piece from Anne Paulson indicates, have elaborated in the spirit of my remarks.

Although my piece in RISKS argued that technology was not all bad, my main goal in life is to convince the technologists to consider the human side of things. There is a tendency to let the technology dominate, forgetting the inconveniences this causes for people. How do I convince anyone? Well, I write, preach, and evangelize. In my consulting, my entire emphasis is on ways of understanding the needs of the users, and then finding ways to bend the technology to fit the people (instead of the other way around).

Consider Paulson's point, that designers of traffic lights (intersections and traffic flow) do not properly consider pedestrians and bicyclists. Actually, I think she underestimated the problem: I suspect these designers consider pedestrians and bicyclists a nuisance that are best gotten rid of. The best approach I ever saw to these concerns was in a letter to the editor in a local newspaper. The author asked why we had "pedestrian crossings" at streets. Shouldn't pedestrians come first? We should have "car crossings." That is,

the pedestrian should automatically be considered to have the right of way, and cars would have to have special places where they could cross the pedestrian stream. The same argument goes for bicycles.

Paulson concludes by saying: "I would be happy to hear from Donald Norman, or other people working or consulting for companies that are designing "drive-by-wire" systems, on how such systems will allow for cyclists." That isn't the right approach. The correct approach is to change the entire mindset of the city planners and people who purchase these devices to put in the proper emphasis. The engineers and designers are often very good, with proper motives, but they can't overcome the mindset of cities that compute traffic flow, and purchase from the lowest bidder -- even if the equipment thus purchased is inferior and the system considerations neglected.

[In addition, I think that automobiles, bicycles, and pedestrians have such different characteristics that they simply should not be in the same traffic streams. We need special bicycle ways (separated from roadways by more than a painted line) and special walkways. (Some European cities -- especially Scandavian cities -- seem to take this approach.) And we should separate different kinds of vehicles as well. And as we get more and more elderly drivers who tend to drive slowly, we will need either efficient point-to-point mass transit or special driving lanes for these elderly "super cautious" drivers (reaction and decision times slow with age, and attention is limited, with less ability to divide attention among several tasks. Those of us in the attention business sometimes say that the elderly have "less attentional resources".)]

The problem faced by RISK readers, designers, and users, is that society puts cost and efficiency first, and cost and efficiency are measured by local, monetary variables. Real cost and efficiency would take into account accident rate, long-term pollution, long term recycling, long-term learning, and employee comfort and job satisfaction. In the end, I think proper attention to these factors increases morale, decreases sickness, increases efficiency, lowers turnover (which thereby lowers training costs), and lowers the cost of cleanup and technological fixes by society. But society is driven by short-term views. It will be hard to change this mindset. But I am optimistic.

Don Norman, Department of Cognitive Science D-015, University of California, San Diego, La Jolla, California 92093 USA

---

## **✉ Re: Autopilots**

*Brinton Cooper <abc@BRL.MIL>  
Wed, 23 Aug 89 16:50:23 EDT*

mrotenberg@cdp.uucp quotes a recent article by Carl Levin. Briefly,

"Airlines are starting to fly a new generation of highly automated jets, raising concerns among safety researchers that pilots will rely too much on the technology and will lose or never learn the sharp skills and

reflexes needed in emergencies."

Most of the article quotes the fears of "experts" and cites recent examples where a pilot's skill overcame emergency conditions, saving many lives. However, the article does not objectively cite balancing situations in which automated systems handled sets of conditions that were too complex and changing too fast for humans ever to respond satisfactorily.

The article includes an irrelevant reference to the old saw that calculators prevent pupils from learning the "basic principles of mathematics," neglecting the fact that one does not do "mathematics" on calculators. One does "arithmetic" on calculators!

Only near the end of the article are cockpit simulators discussed.

"A pilot in a simulator can practice flying after losing various computer and control systems...Still, while simulator training could help for some kinds of emergencies, others... are considered so remote that pilots do not train for them on simulators."

One wonders, "Why not?" Can the great minds of the aircraft industry not postulate virtually any kind of emergency? Can not the simulators be designed/programmed to handle any kind of emergency? This sounds very much like a failure of will, not of ability.

Much of the problem expressed is not new. For years, the US Air Force has been flying high performance tactical jets using significant amounts of automation. If the automated system fails, the game is over. The demands made upon the pilot/airplane system are too demanding ever to be met by humans. These pilots are among the best in the world, and their training heavily depends upon cockpit simulators.

The entire article is a good example of the warped treatment afforded a complex, scientific topic by the popular press. That example, how the public is told about these issues, is probably the best contribution made by such an article to the dialog in the Risks Digest. Perhaps, instead of writing to one another so much, the well-informed among us might write to such as the NY Times, giving more accurate pictures of the issues.

\_Brint

---

## **✉ Re: Automated Highways**

*"George H. Feil" <gf08+@andrew.cmu.edu>  
Wed, 23 Aug 89 10:57:54 -0400 (EDT)*

After reading much discussion on the subject, I'd like to call to attention the cancelled "Skybus" project that would have replaced the old streetcar lines in Pittsburgh. [A feature story on the subject was aired on KDKA-TV Eyewitness News last night; some of the facts presented here came out of the story.]

20 years ago, Westinghouse designed and built a prototype "Skybus" system, which involved driverless, electric rubber-tire vehicles on an exclusive track.

This system was billed as being the cheapest and most efficient public transportation system available. However, many politicians and citizens were opposed to the idea of robot vehicles operating on tracks, "not being able to tell whether an object on the road is a newspaper, a concrete block, or a human body". Of course, this doesn't take into account the fact that the roads were elevated and, for the most part, isolated from the rest of the world.

As a result of the public hysteria, the system was canned, and the new LRV system was built, at five times the cost of Skybus.

There is no doubt in my mind that such a system can and will work, with the proper safeguards taken into account. By isolating the track, there is little need to risk collision with humans, although there would be a need to scan for foreign objects that could serve as obstacles. As for the spacing and switching of vehicles, this is already an automated function for many railroads. What recent railroad accidents can be directly blamed on computer failure?

The point of this story is that the problem can go both ways. We can easily get burned by relying too much on automated systems that can be prone to failure. By the same token, we can get burned economically by refusing a technological advancement that might present a few risks, but at the same time would solve many others (as I feel the Skybus project would have done).

In fact, since then, Westinghouse has teamed up with a German firm (the name evades me at the moment), and has implemented Skybus-like systems in many locations, including Morgantown, WV. In fact, the new mid-field terminal at Greater Pitt. Intl. Airport will be implementing such a system when the terminal opens in '92.

George (HAL) Feil, Carnegie -Mellon University bitnet: gf08%andrew@CMCCVB

---

### **✂ Roads made safer or not?**

*"Pete Lucas - NERC Computer Services U.K." <PJML@ibma.nerc-wallingford.ac.uk>  
Wed, 23 Aug 89 09:31:08 BST*

`Drive-by-wire' - YES i agree that the `human controlled' system causes fatalities at an unacceptable level - YES i agree that the druggies/alcoholics should be kept off the roads, YES i agree that there is a place for civilised public transport (tramcars, buses) and YES i agree that theres a place for automated navigation systems. BUT i don't think they will solve the worlds transport problems. Most journeys (in Europe at least) are of less than 10 miles - taking the kids to school, collecting groceries, popping out for a pizza, and it is the case in the UK that most accidents happen within 5 miles of your home. These are the very situations where the `blocks' of automated vehicles travelling close up, just will not work - they are in most cases urban areas with too many hazards (stop lights, school buses, intersections).

The instances when the bunched, automatic vehicles WOULD be of use are on long-distance journeys. Paradoxically, on a basis of fatalities per thousand miles, the motorways, autobahns and autoroutes of Europe are the safest roads.

For the long journeys, there are trains and planes. Having only been to the States once, and only driven on minor roads, i can't really get a feel for Stateside freeway conditions. But how can a `civilised' country have a 55MPH limit?

Come over to Europe, drive round the London orbital motorway (where the speed limit is 70MPH, but the police turn a blind eye to anybody doing less than 100) and sharpen up your driving skills! The human brain, if it is working properly, is still the best real-time adaptive guidance system we have. Whats more, it comes fitted as a standard, no-cost feature in most people. Its catastrophic failures are thankfully rare, and if it does suffer one, then you aren't going to be worrying any more in any case!

Pete L.

---

### **✂ Training & Software Engineering, a reply...**

*"Edward A. Ranzenbach" <Ranzenbach@DOCKMASTER.NCSC.MIL>  
Wed, 23 Aug 89 13:30 EDT*

I would like to echo some of the sentiment expressed by Tim Shimeall in [RISKS 9.13](#).

I am a non-degreed "software engineer". I started programming as a kid in 1968 and although the term was not used at that time, I was a "hacker". After graduating high school in the early seventies I began attending a community college, the best that I could afford. Unfortunately the draft was on and when I got that compelling notice I enlisted. I honed my craft while in the service, bypassing the service's programmers school because of very high test scores. Within six months, I was appointed the system administrator at a scientific research and development facility. When not handling system matters I was tasked with helping others with their debugging problems. Interestingly enough, there were very few "uneducated" enlisted folk at this site and most of the college trained junior officers were my best clients. They could not program their way out of the proverbial paper bag. When I decided to leave the service, it was decided that my job would be converted to a GS civilian slot. I applied for the job and was turned down because of my lack of a college degree. The base personnel office told me that I was unqualified for a job that I had been doing so well that I was recommended by my supervisor and selected for commendations, as well as NCO of the quarter. I eventually went to work for a large computer vendor who sold me back to the Government to fill my old job. They got \$100,000/year for my services and the facility management people who I worked for as an NCO were thrilled with my encore performance.

In the past twelve years in this business I have held the following titles:

Computer Programming Specialist, Systems Analyst, Senior Systems Analyst, Associate Software Engineer, Software Engineer, Senior Software Engineer, Principal Software Engineer, Computer Security Engineer, Systems Engineer, Senior Computer Scientist.

I have always felt proud of the work that I have accomplished. I am a

published author and have attended invitational conferences. I have always been employed based on my reputation, not on my formal education. I have managed people with far more formal education (and less talent) than I.

I have tried to obtain a degree over the last twelve years but it has not been an easy road. My work has caused me to travel a great deal and to relocate often. At one point I was asked to work abroad for a couple of years. Each time I have moved I have attempted to matriculate to a new university only to lose a substantial number of credit hours to a version of the "not invented here" syndrome. This has made obtaining my "credentials" not only near impossible by very costly. I have taken three different courses in "operating system design" from three different schools and gotten an "A" each time. In one course I corrected the professor's misstatements (discreetly of course) about the operation of the virtual memory demand paging algorithms of a system that I helped to maintain. Don't get me wrong, I feel that formal education is a worthwhile experience. But, for those who must pursue this science without the benefit of a college education, self education is a viable alternative.

I think the software engineering community places too much stock in formal education and not enough in the proven ability to do the job. As Mr. Shimeall pointed out in [RISKS-9.13](#), apprenticeship has long been recognized in this country as an extremely reliable measurement of one's ability to perform. An office mate of mine who holds an advanced degree in computer engineering once told me that obtaining a degree just proved that you could "play the game".

I apologize for the personal nature of this transaction but Mr. Jones' comments brought to a head the frustration that I have felt for a number of years. It seems that people in this field are more interested in where you went to school than in what your opinions on various design issues are. I remember an incident a couple of years ago when I submitted a paper to a conference. It was reviewed and I received a letter of acceptance in the mail along with a request for a biography to be published with the paper. Shortly after sending my biography I received a curt reply explaining that my paper was being dropped from the schedule and would not be published. The explanation was that this was a "professional" conference and surely I would understand. My protests went unanswered. I was recently rejected voting membership to the IEEE because they questioned my professional status because I was non-degreed.

I guess my point is here is that the degree doesn't make the engineer...  
-ear



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

**Volume 9: Issue 18**

**Monday 28 August 1989**

## Contents

- [Proposal for SDI software center](#)  
[Gary Chapman](#)
- [Computerworld article on high-tech weapons](#)  
[George Entenman](#)
- [CHAOSNet used in `SNUFF' snuff](#)  
[PGN](#)
- [DMV records, and individual privacy and safety](#)  
[PGN](#)
- [Another vehicle guidance system](#)  
[Pete Lucas](#)
- [Medics touch computers?!?](#)  
[Sam Bassett](#)
- [Unfounded fault-probability claims](#)  
[Dieter Muller](#)
- [Lowest-bidder or weak specs?](#)  
[David A Honig](#)
- [Automated roads, drive-by-wire, bicycles, and the elderly](#)  
[PGN](#)
- [The Guardian vs computer passwords](#)  
[Brian Foster](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **✉ Proposal for SDI software center**

*Gary Chapman* <[chapman@csl.stanford.edu](mailto:chapman@csl.stanford.edu)>

*Mon, 28 Aug 89 17:58:15 PDT*

This is an item from the newsletter *Advanced Military Computing*, 8/28/89, p.6:

Strategic Defense Initiative managers wrestling with the computer aspects of nuclear war plan to develop a Strategic Defense System software center to meet their application needs.

"If there is an Achilles heel to SDI, it is the critique that we can't make all

the software work; if we do get it to work, it may not work right; it won't be reliable; and it will cost millions of dollars and comprise millions of lines of code," said Lloyd Acker, associate department head National Testbed Systems for the MITRE Corporation.

Acker expects the center to be fully operational by 1991. He said identification of the center's software engineering environment requirements should be completed this year with early prototypes identified and in development.

He said the software center, which get off the ground soon, can help reduce SDI software development risks as well as improve software productivity, integrity, integration, security, practices, standards, and training.

Acker said the software center would:

- \* Be a training center for software managers and engineers. "A significant turnover in experienced software managerial and engineering personnel can be expected in the next decade, while software engineering practices will undergo rapid change."
- \* Exhibit software engineering environments to include tools supporting methods and standards, and serve as a testbed for SDS software quality.
- \* Be a research center for software technologies suited to the SDS mission. Acker said some of the areas of research include parallel processing, neural networks, object-oriented programming, and expert systems.
- \* Track the technology development in other programs that could have an effect on SDI including those of DARPA, NASA, Software Engineering Institute, industry, and academia.
- \* Be a trusted repository for SDS software as it is validated and certified. An early focus will be how to prevent the injection of computer viruses into the system.

-----

Jeez, where have I heard all this before? I thought this was what the National Test Facility in Colorado Springs was supposed to be doing. Now we're going to build something with an identical mission, a facility which will do world-class research on parallel processing, neural networks, object-oriented programming, and expert systems to boot. Sounds like yet another SDI boondoggle to me.

The center will "Be a trusted repository for SDS software as it is validated and certified." How do they expect to do this?

"An early focus will be how to prevent the injection of computer viruses into the system." If this center has to be built, it would seem to me that a more reasonable place to start would be to figure out whether the SDI makes any sense at all, or whether it's just a screwball idea designed to "bucket brigade" taxpayer money to defense contractors and think tanks like MITRE. Who

cares if there are viruses in something that's not designed to actually "work"?

Gary Chapman, Executive Director, Computer Professionals for Social Responsibility

---

### **✂ Computerworld article on high-tech weapons**

*George Entenman <ge@mcnc.org>*

*Fri, 25 Aug 89 10:07:11 EDT*

Risks readers should be interested in an article in COMPUTERWORLD (August 21, 1989, Vol. XXIII, No. 34, page 1) by James Daly of the CW staff entitled "High-tech weapons, low-tech GIs". The article contains few surprises for readers of this newsgroup, but it neatly summarizes many of the risks associated with computerized weaponry.

The article's main thesis:

Despite the investment of huge amounts of training time, effort and money, some critics argue that today's super-sophisticated armaments have become so complicated that they have outgrown the ability of sailors and soldiers to use them effectively.

It also explains why we may be irrevocably stuck with high-tech weapons:

Reports ranging from a B-1 bomber crashing when it hit a pelican to the embarrassing Divad project -- a computer-operated anti-aircraft gun that once identified a rotating latrine fan as the closest threatening target -- have initiated brass-filled investigative hearings.... The trouble is, the military culture may already be too infatuated with leading-edge devices to ever turn back.... [The] Pentagon's electronics procurements have more than tripled since the beginning of the decade and now account for more than 40% of the military's production costs.

The Pentagon's "solution":

Because the list of the Pentagon's high-tech goof-ups is long, the Defense Department has begun to seriously investigate the use of artificial intelligence.

---

### **✂ CHAOSNet used in `SNUFF' snuff**

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

*Thu, 24 Aug 1989 10:44:34 PDT*

Undercover police in San Jose, California, have been tracking BBOARDS for several years, looking for computer users who boasted about their criminal exploits. It was such activity that led them to Virginians Dean Ashley Lambey, 34, and Daniel T. Depew, 28, who have been accused of conspiring to kidnap a young boy to be filmed as they molested him and then killed him. [Source: San Francisco Chronicle, 24 August 1989, article by Tracie L. Thompson]

---

## ✂ DMV records, and individual privacy and safety

Peter Neumann <neumann@csl.sri.com>

Sun, 27 Aug 1989 11:30:04 PDT

In previous installments in RISKS, we have discussed the relatively open availability of the database of the California Division of Motor Vehicles. In response to the July 18 murder of actress Rebecca Schaeffer by someone who tracked her down through DMV records (via an Arizona private investigator), Gov. George Deukmejian has directed the DMV to restrict release of information, to protect individual privacy and safety. (The DMV had 41 million requests in 1988, mostly seemingly business related.) New rules take place 1 Oct. They require bulk users to register and sign restrictive agreements, and impose a 10-day delay on the response in certain cases. The current practice of notifying the driver when an individual request is made will thus give the driver a little warning before the record is mailed out. (DMV information is all public record info, but the home addresses of certain drivers -- judges, law-enforcement officers, etc. -- are supposedly not released. Whether they are actually on-line but suppressed by the system is another matter.)

---

## ✂ Another vehicle guidance system (Pete Lucas)

"Pete Lucas - NERC Computer Services U.K." <PJML@ibma.nerc-wallingford.ac.uk>

Fri, 25 Aug 89 16:16:22 BST

More on vehicle guidance: The following is summarised from an article in 'Personal Computer World' september 1989.

A description is given of a system called AUTOGUIDE, being developed by the Transport and Road Research Laboratory (TRRL) near Reading, England.

The pilot system uses a digitised map of the area concerned, and a set of 'beacons' (which use an infra-red digital link to inform passing vehicles of their position, and local traffic conditions).

Passing vehicles presumably 'poll' the beacons which respond by sending data.

Information ('Take the next left', 'Road closed at intersection') is displayed on an alphanumeric LCD display on the vehicle instrument panel.

Information from the beacons is relayed back to a central computer which is able to compute vehicle speed by the time taken for individual cars to pass between the beacons. In this way, the central computer can identify congested areas as the congestion develops, and be able to determine alternate routes.

Siemens, Logica, GEC and Plessey are all involved in the development of the system, the RAC and AA (both British motoring organisations) are also part of the various consortia doing the development. The British government are currently deciding on which consortium to choose to award the pilot study project to. Initially, around 300 beacons are likely to be needed in an area the size of London, at an estimated cost of 5 to 10 million UK pounds.

Possible things to consider as potential risks with such a system::

- 1) Such a system COULD be made to identify individual vehicles, hence allowing the authorities to 'track' individuals as they drive around cities.  
Civil liberties people will no doubt have some comments on this indirect 'electronic tagging'.
- 2) Since the system can 'divert' traffic, there is a risk that residents who suddenly find a high-speed stream of vehicles diverted down their normally quiet streets and may get somewhat uptight about it.
- 3) I dont know about the details, but it sounds like such a system could be easily tampered with. Criminals who wished to could, for example, operate a very powerful beacon and create either congestion or open roads to foil police chases. Anyone remember the film 'The Italian Job' in which the robbers crashed a trafficlight computer to cover their escape by creating traffic chaos?
- 4) Governments/city authorities could 'fiddle' the system to give an unfair advantage to public transport by unethical means - make the roads \*APPEAR\* more congested whilst creating congestion-free zones for buses.

Pete L.

---

### **⚡ Medics touch computers?!?**

*Sam Bassett RCD <samlb@pioneer.arc.nasa.gov>  
Thu, 24 Aug 89 00:35:11 PDT*

I was a bit astounded by Brint Cooper's story of medical personnel in the hospital he was consulting for being willing to learn the basics of booting and caring for the computers that held their medical database.

In my experience, this shows an uncommon amount of good sense on the part of the medical personnel, and a sharp departure from the normal behavior of (non-computer-literate) professionals who use computers. One wonders how many gripes there would have been in the Toronto stock exchange if the stockbrokers had been willing to take a similar interest in the machines on which their living depends.

---

### **⚡ Unfounded fault-probability claims**

*Dieter Muller <dworkin@Solbourne.COM>  
Thu, 24 Aug 89 12:48:52 MDT*

In [RISKS 9.17](#), [mentat@walt.cc.utexas.edu](mailto:mentat@walt.cc.utexas.edu) (Robert Dorsett) has a gripe with flight automation:

\* Unfounded fault-probability claims by manufacturer (both in program verification and hardware reliability).

This is not necessarily true. Many aircraft manufacturers believe

they have a very firm foundation for the reliability of their hardware. One of my former employers leases programs for this very purpose. However, these programs are known to have bugs in sections that "no one uses" [read: no one's complained about it being wrong]. Also, in the theoretically working sections, they are using data for components that was out of date 10 years ago. By the way, the justification for all this was that "the numbers are only used for advertising anyway. No one believes them."

So, the manufacturers are reporting in good faith what the reliability software tells them, but the software lies. I was amazed to find out this software producer has never been sued as a result of the software's claiming a product would last X amount of time, when the product actually failed much more often. Maybe no one \*does\* believe the numbers, but it isn't noised about much....

Dieter Muller

---

### ✂ Lowest-bidder or weak specs?

David A Honig <honig@BONNIE.ICS.UCL.EDU>  
Wed, 23 Aug 89 19:37:47 -0700

I have seen at least two incidences of RISKS contributors decrying the fact that they had to deal with systems provided by a "lowest bidder". It seems to me that if the specifications are complete and correct then there should be no problem. And I cannot think of another decent way to buy systems (the next-to-lowest bidder? the highest bidder?) that will solve the problems.

I realize that formal software techniques are considered pie-in-the-sky, and the "iterative design techniques" are what really happens, but isn't the process of analysing and writing specs, and checking that a purchase meets them, a sufficiently important thing?

I know it takes more effort to specify what you \*really\* want and it'll cost more when suppliers give you bids, but at least you're not trusting something you don't want to.

[It was of course John Glenn who commented on how he felt knowing that he was astronauting around in something that was built by the lowest bidder. The real problem is the extent to which corners have been cut so that the contractor does not lose money, or indeed tries to maximize profits. If the "ethic" is that anything goes if you can get away with it, then THAT is a problem. If systems are really built to spec, then you should certainly worry whether the spec was adequate. PGN]

---

### ✂ Automated roads, drive-by-wire, bicycles, and the elderly

Peter Neumann <neumann@csl.sri.com>  
Mon, 28 Aug 1989 18:29:24 PDT

RISKS received a huge flurry of stuff as follow-ups on this topic [singular],

with considerable overlap, as well as second-order and third-order discussion. I'll try to cull out the highlights. Sorry to you contributors who might have thought there was a big black hole out here where RISKS is supposed to be.

By the way, the cutover to the new system and its mailer has improved my life, and has resulted in only a few dropped subscribers. Thanks for your patience.

Your underautomated moderator

---

## **✂ The Guardian vs computer passwords**

<blf@scol.UUCP>

Fri Aug 25 11:15:15 1989

The Guardian newspaper (London, U.K.), Thursday 24th August (reprinted without permission). My comments follow.

Any errors in the transcription are entirely mine (but the Guardian's reputation for poor proofreading is of no help).

-----

A daily changing password is a simple but ridiculously under-used anti-hacker device, argues P. Nath

GIVE US THIS DAY ...

There is a growing acceptance of the view that little can be done to deter hackers, since they have successfully penetrated so-called secure systems including those of the US and Nato commands.

But computer users could take some measures which are ridiculously simple and will only need a couple of minutes each week, to stop more hackers than armies of policeman ever could. These measures could be put into operation immediately and do not involve any new hardware or software.

All computer systems allow information to be protected with passwords, but this facility is not properly exploited. To be effective a password should be unguessable and temporary, and yet most passwords are based on names or addresses familiar to the users, and very seldom, if ever changed. It's like hiding the keys of the house under the doormat in the belief that no burglar will be clever enough to discover them.

The fact that hackers arrange meetings where they exchange, sell and circulate interesting passwords proves that those passwords are not changed often enough. If passwords are selected carefully and changed every two or three days, even the most experienced hackers will find it impossible to discover them.

Although every protection system should be different, some general rules for coining and deploying the passwords can be easily laid down. Perhaps the users may even learn to derive as much thrill in coining

un-hackable passwords as hackers no get in breaking them.

Ideally a password should be based on things which are in no way related to the user or his organisation, and the word should be new, pronounceable and easy to remember.

The easiest method is to start with common names like Mexico, Dublin, France, Durham, London, Moscow, Cyprus etc, and form new words like Icomex, Lindub, and Cowmos by interchanging their first and second halves. A better group of new words can be made by combining halves of different words; for example Lonlin, Frarus, Mexrus and Mosham. Such words become very easy to remember if a large item is paired with a smaller one, and the two are linked in some way.

A better idea is to use two passwords. Easily remember pairs of words may be made up by linking an item with one of its features. For example, the onion domes of Moscow being to mind words like Onimos and Onicow. A pair of words like this can be used interchangeably as passwords, by an individual or a group.

Other members of the group will not be inconvenienced, since even the strictest computer system allows two or three attempts to key-in the password correctly. By just typing Onicow as a guess, a user will happen to be right about half the time. If the computer rejects this word, he is sure to gain access by typing Onimos. This tolerant nature of computers is well exploited by hackers, and there is no reason why users should not take advantage of it as well. Computer users suffer from an irrational fear of forgetting their passwords, so they adopt unforgettable names like those of their wives or children, and sometimes their own names. The idea of a password which changes frequently, say once or twice a week, seems like mental torture, but it is not. The underlying rules for such passwords are so simple the once learnt they become very easy to recall.

Consider a hypothetical international company and imagine that all its salesmen are enjoying a new year party. All the data concerning products and prices are key only in the central computer, the password for which is to be changed every day. The salesmen do not wish to spend more than five minutes to learn the password rules and they insist that no written record of the rules should exist, and that no member should ask or divulge the rules to another member or anyone else. Is it possible for them to invent a totally reliable but unwritten set of rules which will churn out a new password every day?

Yes, and the procedure is quite simple and easy to remember.

To be changeable daily the password must be linked in some way to the calendar, but the information has to be coded in such a way that hackers will not be able to crack it in 24 hours. As a starting point take an uncommon three-letter base word, for example, ULM. This leaves room for three letters or digits to codify the date, for example, Sunday, April 30. This day is in the 17th week of the year, is the 120th day of the year, and is 245 days from the end of the year. The password can be any of the following:

ULM30S (30th, Sunday)  
ULM30A (30th, April)  
ULM304 (30th, April)  
ULM430 (April, 30th)  
ULM17S (17th week, April)  
ULM301 (30th, Sunday) (1=Sun, 2=Mon, 3=Tue etc)  
ULM125 (difference between 245 and 120)

and so on.

These passwords may be modified by taking the code letters for days and months from another language (for example, German) or by adding a fixed number to the digits relating to dates and months; or by multiplying these digits by a 2 or 3; or by writing them differently, for example in an octal base.

Other combinations can be obtained by putting the calendar information inside the word. ULM30S can be written as UL30SM or U30LMS or U30LSM. Reversing this order provides another set of words.

The attraction of such a system is that although the users have to agree on only one of these simple rules and remember it for a year (assuming the system is renewed annually), the hacker will need, if he is very lucky, hundreds of trials to find out how the daily information has been encoded and 24 hours will not be long enough to do this.

If by some miracle a hacker breaks the daily code, he still has to discover the fixed letters U L M in their correct order, and this task will need thousands of additional trials. By that time he may decide to give up hacking as a bad job.

-----

Whilst this column gives some good advice (e.g., "a password should be unguessable and temporary"), reasonable suggestions for choosing decent passwords (e.g., invention of "Onicow"), and implies other sensible precautions (e.g., no written records or disclosure), it is flawed.

Ignoring the factual errors (passwords exist only on MS-DOS via add-on products; ergo, new software and/or hardware may be required), it omits several key points. The most obvious omission, perhaps, is that with the ULM scheme the rules must be changed everytime a salesman leaves the company. (If the information is so valuable to require daily passwords, then it would be unacceptable for any former employee to still effectively know the password.) For the type of company described, this could be rather frequent, presenting the problem of how to distribute the new scheme (which is, quite sensibly, neither written down nor ever divulged).

The column also supposes that unauthorised agents (called "hackers", but I refrain from that debate) gain access only by guessing passwords. I suspect that such (random) guessing is the among the rarest attacks. (But the problems with short passwords and restricted alphabets are hinted at.)

Assuming that the passwords control the ability to log onto the system (i.e., authenticate system access) then the implication that passwords should be shared (amongst all the salespeople, in the ULM example) is a disaster. Shared passwords imply shared accounts, which frustrates any concept of accountability -- since no one is individually responsible (for a shared account), a breach cannot be traced back (assuming some auditing facilities exist) to an individual person actions or inactions.

It is good to see passwords discussed in the mainstream press, and even better when the discussion includes sound instruction. But it unfortunate that the discussion is so flawed that the good points are overlooked.

Brian Foster, SCO Trusted UNIX Project, The Santa Cruz Operation, Ltd., London

[We have also mentioned in past issues the risks that the passwords may be stored unencrypted in accessible places, may be transmitted unencrypted via easily readable transmission media, and that passwords are intrinsically vulnerable. But you should not be surprised to see a technical topic mauled in the press... 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 9: Issue 19

Wednesday 30 August 1989

## Contents

- [NEW INSTRUCTIONS TO FTP VOL i ISSUE j, effective immediately](#)  
[PGN](#)
- [Reg. of Motor Vehicles computer slows down](#)  
[Adam Gaffin](#)
- [British nuclear reactor software safety disputed](#)  
[Jon Jacky](#)
- [South German hackers hack TV German Post](#)  
[Klaus Brunstein](#)
- [Ethics](#)  
[Donald J. Weinshank via Tom Thomson](#)
- [sci.aeronautics, a new newsgroup](#)  
[Robert Dorsett](#)
- [What's a stamp? \(postal service problems\)](#)  
[David Elliott](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✉ NEW INSTRUCTIONS TO FTP VOL i ISSUE j, effective immediately

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

*Thu, 24 Aug 1989 10:44:34 PDT*

ftp CRVAX.sri.com

anonymous

---

### ✉ Reg. of Motor Vehicles computer slows down

*Adam Gaffin* <[adamg@well.UUCP](mailto:adamg@well.UUCP)>

*Wed, 30 Aug 89 10:54:54 pdt*

From the Middlesex News, Framingham, Mass, Aug. 29, 1989

By Michael Sereda

NEWS STAFF WRITER

MetroWest police, more accustomed to battling crime, are battling a broken

Registry of Motor Vehicles computer that hasn't spit out information since Sunday. So far, 6,000 inquiries on licenses and registrations have backed up, handcuffing police and leaving Registry officials to crank out renewals on paper.

"It's a real pain in the neck, particularly on a busy night and there's so much going on," said Medfield Police Dispatcher Shirley Rossi. "You're able to check the status of someone on a warrant ... but you can't check the status if they have a suspended or revoked license, and you can't check the status of a vehicle, if it's unregistered, registered. It just basically makes it difficult if they want to write a ticket." "This is an ongoing thing with (the Registry)," Rossi said.

Trouble began, spokesman Kathi Connelly said, on Sunday morning when the Registry shut down the electronic brain for four hours of scheduled maintenance. After the maintenance was performed, the computer came back on line for about an hour and then started acting up, she said. The 4-year-old computer, which stores information on the state's 3 million drivers and 6 million vehicles, was operating off and on throughout Sunday, before "crashing" late that night or early Monday morning, she said.

The glitch meant that police throughout the state could not check on a person's driving record or the validity of a registration. "It gets very difficult," said Framingham Lt. Wayne McCarthy. "There've been several times that it's down, and later it comes up (after a suspect is let go) and it comes back that someone's license is revoked or suspended. "They may have had a license on them and we couldn't check on it," McCarthy said.

"It kind of stops the checking process out on the road," said State Police Sgt. Joseph Parmakian.

While the computer was down Sunday and Monday, the system automatically stored the inquiries and answered them when operation resumed between 4 p.m. and 6 p.m. Monday, Connelly said.

At the Registry, customers who wanted to renew their licenses went away with temporary paper renewals and without the laminated photo license, which is computer-generated, Connelly said. Those drivers can return for the photo license, she said. She said she could not estimate how many customers might have been inconvenienced. Other Registry transactions involving the public were done on paper, she said. "To be frank, we were kind of worried that something like this would happen," Connelly said. "The computer has been operating at 100 percent capacity for more than a year. Generally, computer systems are supposed to operate at no more than 85 percent of capacity."

The computer's maker, Amdahl Co. of Sunnyvale, Calif., flew parts and repair technicians to Boston to help out, she said. The repairs did not cost the Registry additional money because they were covered under a maintenance agreement, she said.

Permanent help is on the way for the Registry in the form of a new computer with an expanded memory, Connelly said. The new computer will have the ability to handle 40 million instructions per second - in computer lingo, that means it's real fast. The Registry will be going out to bid in 10 to 12 weeks for the

\$7 million machine. The money for the computer, Connelly noted, has already been budgeted and will be paid over a five-year period.

Connelly said that David Lewis, the Registry's computer boss, "feels secure the problem has been taken care of." "We'll be happy when it's replaced," she added.

---

## British nuclear reactor software safety disputed

Jon Jacky <JON@GAFFER.RAD.WASHINGTON.EDU>

Tue, 29 Aug 1989 14:06:30 PDT

The following article appears in NEW SCIENTIST, 5 August 1989, p. 24:

CEGB Rebuffs Critics of Safety Software by Susan Watts

The Central Electricity Generating Board has responded to critics who doubt the reliability of the software that will protect Britain's latest nuclear power stations from accidents. Specialists in computer safety systems fear that this software does not meet current standards for such "safety-critical" software, published recently by the Ministry of Defence (MoD). The CEGB has been reluctant to publish details of the protective system.

At a special session of the Hinkley Point inquiry in Bristol, Martyn Thomas, the chairman of the committee on safety software at the British Computer Society (BCS), urged the CEGB to allow an expert committee to make an independent assessment of the software. This software, which the board ordered from Westinghouse in the US, might one day be solely responsible for shutting down pressurized-water reactors should something go seriously wrong.

The MoD's draft standard, Def Stan 0055, stipulates that all software for systems which protect human life must be analyzed mathematically, rather than simply relying on estimates of the probability that such software will not fail.

Thomas fears that the systems could not meet the requirements of MoD's new standard (THIS WEEK [a section in NEW SCIENTIST] 1 April 1989). The only way to allay concern about the protection system among computer experts would be for the CEGB to publish details of the system and to allow the expert committee to scrutinize it, he says.

The board rejects charges that the emergence of the new standards invalidates or renders inadequate its designs, which have been under development for some time. The board points out that it has its own independent assessment team, which includes a member of the safety systems group of the BCS.

But Thomas says that this "Independent Design Team", although independent of Westinghouse, is made up of employees of the CEGB. This is not good enough, says Thomas, who wants the inquiry to open an extra session on the safety aspects and reliability of the software which will control the reactor.

In Bristol, Thomas said that the Health and Safety Executive, whose team at the

Nuclear Installations Inspectorate (NII) has to approve the system before it is allowed to operate, is severely short of skilled resources for assessing programmable electronic systems of any sort. He also has serious reservations about whether the NII has the staff and skills to evaluate safety of the protection system.

He says that the CEGB has not answered the substantive point of his evidence; that this important area of the design, where opinions within the computer community have been maturing quite rapidly over the past six months, ought to be examined by public inquiry. He says that he asked the CEGB several months ago for information about the design of the system.

The Health and Safety Executive (HSE) has responded to the evidence submitted by Thomas, and says that it has adequate expertise and resources to do its job. The HSE says that it has addressed the potential problems with software identified at the time of the Sizewell inquiry, and that the NII expects the CEGB to make use of new checking techniques as they become available.

- Jonathan Jacky, University of Washington

---

### **South German hackers hack TV German Post**

*Klaus Brunnstein <brunnstein@rz.informatik.uni-hamburg.dbp.de>  
29 Aug 89 14:16 GMT+0100*

Last Saturday (August 26, 1989), ZDF (=2nd German TV, one of the 2 nationwide TV channels) asked their spectators whether smoking should be banned in the public. The spectators could answer by telephone, dialing for "yes" a telephone number nnnnnn1, or nnnnnn2 for "no". Within a time slot of 14 minutes, 52.942 telephone calls came in, with a quota of 54:46 in favor of a smoking prohibition. That means, that 29.669 voted in favor of a prohibition, and 25.273 opposed.

On Monday (August 28, 1989), a group of South German hackers said that they manipulated the quota by dialing the "yes" number with from 83 PCs at a rate of 4 times a minute; virtually all of their calls came through so that about the maximum of 4.648 Yes-votes came from their computers. The result was thus significantly changed: without the computer votes, the result would be: Yes=25.021; No=25.273, which is a small majority of the opposition.

German news media (only) now start a debate about the "security" (not about the quality!) of the German Post Office's "TED" =TEleDialog system used for this TV transmission. The system was developed in 1979 (and used several times, mainly for entertainment purposes, e.g. vote on the Saturday movie). TED consists of 11 regional computers which count how often a specific number is dialed; the count is transferred to the TV station which rented this service, after a given time limit is reached. The maximum capacity for a nationwide counting procedure is 350.000 "votes" per hour. On Saturday, only slightly over 50% of the capacity was used, probably due to vacation time and missing interest in the corresponding TV show.

The system can easily be hacked; probably, some more hackers tried and practised such hacks earlier. There have been some discussions before when, at a local election in the Federal State of Hamburg, some strange results about political themes came up. But only now, as leisure time themes and activities of hackers are involved (and other catastrophe themes are not visible), a discussion is started about the "security". My prognosis: the essential question about the quality of the results produced by such a tool and procedure will only be discussed when questions of common (national?) interest are asked, such as: shall we replay Steffi's or Boris's last winning game.

Klaus Brunnstein      Hamburg, FR Germany

---

## ✂ Ethics

*Tom Thomson <tom@prg.oxford.ac.uk>*

*Tue, 29 Aug 89 12:57:36 bst*

I thought this article from humanist was worth posting to risks and to security. What risks do we suffer if our engineers/scientists are unethical, or are taught to subscribe to conflicting sets of ethical principles? Is it likely that societies like ACM, BCS, IEEE, etc will have incompatible ethical codes, each of course incompatible with whatever is taught in the computer science schools? Forwarded article:-

Sender: HUMANIST Discussion <HUMANIST@EARN.UTORONTO>  
Reply-To: Willard McCarty <MCCARTY@CA.UTORONTO.EPAS.VM>  
Humanist Discussion Group, Vol. 3, No. 402. Monday, 28 Aug 1989.

Date: Mon, 28 Aug 89 17:14:47 EDT  
>From: weinshan@cpswh.cps.msu.edu (Dr Donald J. Weinshank)

If I may, I would like to reopen the question of "computer ethics." Let me try to formulate the question this way: "Is there a rational and consensual basis for computer ethics?"

The older I get, the more I feel the poignancy of this exchange in The Brothers Karamazov:

"Is that really your conviction as to the consequences of the disappearance of the faith in immortality?" the elder asked Ivan suddenly.

"Yes. That was my contention. There is no virtue if there is no immortality."

Absent a consensual reality, on what basis can we construct a system of computer ethics for our students?

Do we reduce ethical questions to the merely legal ones? If it ain't illegal, is it OK?

Do we point to a series of mini-consensuses? The ACM says ....., and the MLA says ....., and the Department of Redundancy Department has published yet another statement of computer ethics. Are students to choose one ethics position from Column A and one from Column B as they see fit?

Are computer ethics merely negative ("Thou shalt not..."), or are they also positive? Are there ethical statements which are unique to (or apply with special force to) the field of computing, or are they the general ones of "intellectual honesty, curiosity, an eye for detail, a respect for theory, and delight at discovery" (Miller quoting Ryle on 20 June, 1989).

If computer ethics can be taught, then I have these questions:

- \* Who is doing the teaching? People in the Humanities? Engineers? Computer Scientists?
- \* What are the people who are teaching computer/engineering/scientific ethics teaching?
- \* What texts?
- \* What contexts: part of many courses or a separate required/elective course?

---

### **sci.aeronautics, a new newsgroup**

Robert Dorsett <rd@rascal.ics.UTEXAS.EDU>  
Wed, 30 Aug 89 19:41:02 CDT

The sci.aeronautics newsgroup has been formed on usenet. It will be dedicated to discussions of various aspects of aviation, such as human factors, airliner operations, avionics, and aerodynamics. It is intended to complement the existing rec.aviation newsgroup, not replace it.

There is also a mailing list. Submissions should be mailed to  
aeronautics@rascal.ics.utexas.edu  
Administrative details (requests to subscribe, unsubscribe, questions) should be addressed to:  
aeronautics-request@rascal.ics.utexas.edu

The "aeronautics" mailing list will be a moderated version of the sci.aeronautics newsgroup. It will be a one-way feed (sci.aeronautics -> mailing list), unless sufficient demand requires that it go in the opposite direction.

Robert Dorsett                      Internet: rdd@rascal.ics.utexas.edu  
UUCP: ...cs.utexas.edu!rascal.ics.utexas.edu!rdd

---

### **What's a stamp? (postal service problems)**

David Elliott <dce@Solbourne.COM>  
Tue, 29 Aug 89 10:05:35 -0600

Recent articles and letters in "Linn's", a weekly philatelic newspaper, give an interesting view of problems in the US Postal Service.

A recent scam has people paying as much as \$40 to find out about a "little-known regulation" that allows people to send first-class mail for \$.02 instead of \$.25. There is no such regulation, at least not specifically.

Nowadays, stamps are printed with phosphorescent inks (sometimes the colored ink contains phosphor and sometimes a clear overcoating is applied). Automatic cancelling machines detect the phosphor, rejecting envelopes that have none.

The result is that any stamp with the phosphor will trigger the cancelling machine: a \$.25 stamp, a \$.02 stamp, a \$.01 stamp, a piece of selvage (stamp sheet edge), some used stamps, and some foreign stamps. In fact, one political candidate's secretary used this trick to "save money". No charges were made ("It's a simple mistake").

On the other side of the coin (as it were), overzealous postal clerks refuse valid stamps:

- \* The 1987 Stamp Collecting issue, which shows a 100-year old cancel as part of the design ("We don't accept cancelled stamps").
- \* The 1947 100th anniversary souvenir sheet contains stamps with the same designs as the US 1847 issues (5 and 10 cent values). The 1847 stamps were invalidated during the Civil War.
- \* The 1989 souvenir sheet showing a reprint of the 90 cent Lincoln stamp of the 1880's is expected to have similar problems.
- \* Any postal customer with the proper permit is allowed to use precancelled and fractional-valued stamps, but obtaining and using the permit is not always possible with some clerks and postmasters.

David Elliott



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 9: Issue 20

Friday 1 September 1989

## Contents

- [Last Night's "Tonight" was Unknighted; Cars on Carson Top Hat Trick](#)  
[PGN](#)
- [More on the Therac 25 -- by Jon Jacky](#)  
[PGN](#)
- [Witness questions attack on Iranian jet](#)  
[Robert Dorsett](#)
- [Risks of on-line course registration](#)  
[Deborah M. Clawson](#)
- [Specifications](#)  
[Martyn Thomas](#)
- [Re: Lowest-bidder or weak specs?](#)  
[Scott](#)  
[Robert Hirsch](#)  
[Bill Cattey](#)
- [Pilot simulator training and boredom](#)  
[Dan Franklin](#)
- [More on automation](#)  
[Robert Dorsett](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **✉ Last Night's "Tonight" was Unknighted; Cars on Carson Top Hat Trick**

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

*Fri, 1 Sep 1989 11:00:36 PDT*

On 31 August Johnny Carson did an impression of Abe Lincoln as a budding young standup comic, wearing a two-foot top-hat. The end of the skit involved triggering a radio-controlled device that blew the hat upwards off of his head. A long delay arose during the taping of the show when the hat kept blowing off Johnny's head backstage before his entrance. His technicians figured out that RF interference from nearby kids with remote-control robot cars kept triggering the hat. The obvious solution was to get the kids to stop transmitting during the skit. Honest, Abe had some good lines, but Johnny's hair-raising gimmick top-hatted them all.

---

## ✦ More on the Therac 25 -- by Jon Jacky

Peter Neumann <neumann@csl.sri.com>

Fri, 1 Sep 1989 11:06:32 PDT

There is a very nice article by Jonathan Jacky entitled "Programmed for Disaster, Software Errors That Imperial Lives", in THE SCIENCES, the bimonthly of The New York Academy of Sciences, September/October 1989. Jon gives an in-depth analysis of the Therac 25 case. (The credit line notes that Jon is currently designing software for a computer-controlled radiation-therapy machine.)

---

## ✦ Witness questions attack on Iranian jet

Robert Dorsett <rd@rascal.ics.UTEXAS.EDU>

Fri, 1 Sep 89 12:00:00 CDT

By George C. Wilson  
Washington Post Service

The USS Vincennes, which shot down a civilian airliner in the Persian Gulf on July 3, 1988, killing 290 people, had gained a reputation for being an overly aggressive "robo-cruiser" and probably provoked the sea battle with Iranian gunboats which preceded the shootdown, according to a commander of a ship on the scene at the time.

Writing in the September issue of the US Naval Institute magazine *Proceedings*, Commander David Carlson said the radar on his ship, the USS Sides, a patrol and escort frigate, showed that the airliner was climbing in a non-threatening way inside the designated commercial airline corridor.

He said he would not have ordered his own crew to fire missiles at the plane, as did Captain Will Rogers III, skipper of the Vincennes.

In another part of his remarkably frank account, which is likely to refuel controversy generated by the shootdown, Carlson wrote that the Vincennes started the sea battle in response to what may have been nothing more than warning shots from Iranian gunboats feeling threatened by the cruiser's helicopter.

Having watched the performance of the Vincennes for a month before the incident," Carlson wrote, "my impression was clearly that an atmosphere of restraint was not her long suit. Her actions appeared to be consistently aggressive and had become a topic of wardroom conversation. "Who's driving the problem in Vincennes?" was a question asked on numerous occasions prior to 3 July.

"'Robo-cruiser' was the unamusing nickname that someone jokingly came up with her, and it stuck," Carlson said. My guess was that the crew of the Vincennes felt a need to prove the viability of Aegis (the highly sophisticated anti-aircraft system on the cruiser) in the Persian Gulf, and that they hankered for an opportunity to show their stuff..."

The Vincennes crew misidentified the civilian airliner as an Iranian F-14 fighter plane, which does not carry anti-ship weapons, and shot it down with missiles, to the horror of Carlson watching the same plane on radar.

"We locked up and illuminated" the approaching Iranian airliner "with our missile fire control radar," Carlson wrote. "The aircraft continued climbing on a southwesterly course that would take it directly over the Vincennes position. Based on closest point of approach to the Sides (range and altitude), lack of any significant known F-14 antisurface warfare capability... lack of detected radar emissions and precedent, I evaluated the track as a non-threat..."

"The Vincennes announced her intentions to take TN 4131 (Track Number 4131, the Iranian airliner) with missiles at 20 miles. I wondered aloud in disbelief, but I did not do the one thing that might have helped. I did not think to push for a re-evaluation of IFF (identification of friend or foe)..."

---

### **✂ Risks of on-line course registration**

*"Deborah M. Clawson" <Clawson@DOCKMASTER.NCSC.MIL>  
Fri, 1 Sep 89 17:01 EDT*

Yesterday the University of Colorado at Boulder newspaper carried an article entitled "Officials say CU keeps records confidential." The article was in reaction to reports that a murderer obtained his former girlfriend's course schedule by giving a University of Washington clerk the victim's Social Security number and name. The point of the article was to assure students that "that couldn't happen here." In interviews CU officials reviewed employee training on the Family Education Rights and Privacy Law and said that reminders about the law are consistently sent out. A course schedule would not be released to anyone other than the student and only if the student had ID. Every one of administrators interviewed was confident that no one else could obtain a student's course schedule.

The RISK involved is that no one seems to have thought about our on-line course registration system. This system allows a student to review his or her schedule by phone. And what do you need to access that information? The student's Social Security number and a secret PIN.

Unfortunately, the PIN is assigned as the student's birthdate...

---

### **✂ specifications**

*Martyn Thomas <mct@praxis.UUCP>  
Thu, 31 Aug 89 18:58:29 BST*

>From: David A Honig <honig@BONNIE.ICS.UCI.EDU> [writing in RISKS]  
>It seems to me that if the specifications are complete and correct then  
>there should be no problem.

It seems to me that much of the grief in our industry, and many of the risks, stem from the assumption that every system has an "a priori" specification, if only you can find the right person to ask. In my experience, specifications change as people understand the implications of what they have asked for. Specifications also change because new ideas come along, or the users change, or the constraints change.

Most of all, specifications change because every useful system mirrors the real world in some aspect, and the real world changes. So specifications (in the sense of \*real, current needs\* ) change throughout the development of any useful system and throughout its service life, too.

This is why "lowest compliant, fixed-price bid" is a poor way of purchasing systems.

---

**✉ Re: Lowest-bidder or weak specs? (David A Honig, [RISKS-9.18](#))**

<[scott@cs.rochester.edu](mailto:scott@cs.rochester.edu)>

Tue, 29 Aug 89 09:33:08 EDT

How about "most trusted bidder with a reasonable price"? The problem with many lowest bidder schemes (particularly those often legislated by well-meaning government bodies) is that they do not provide an adequate mechanism to separate competent bidders from incompetent bidders. What good are detailed specifications if you don't honestly believe that the contractor will be able to meet them, or if you believe you're going to have to pay enormous legal fees to force the contractor to meet them? There's plenty of opportunity for abuse if you let public officials hire their "favorite" contractor regardless of price, but a pure lowest bidder scheme is not the solution, either.

---

**✉ Re: Lowest Bidders ([RISKS-9.18](#))**

Robert Hirsch- RCE <[hirsch@pioneer.arc.nasa.gov](mailto:hirsch@pioneer.arc.nasa.gov)>

Tue, 29 Aug 89 09:54:24 PDT

A somewhat jaundiced view of the process from the viewpoint of an employee of several large and small contractors (who shall remain nameless) is that first of all, the going practice seems to be to ask the developers what it will cost to develop a system to the spec provided, then say "no, try again" to realistic estimates until the bid comes down to less than the program office believes the competition will bid. The same, of course, applies to schedule. In short, it's a low-ball contest with the award going to whoever makes the most audacious bid.

Next comes the engineering challenge of devising an implementation which can be done in the time and budget which was bid, and which can somehow be construed as meeting the requirement. A specification calling for on-line error diagnostics may be met by having the terminal beep, or some such travesty.

Of course, there is the problem of divining what the spec does ask for. I have been at a design review where our customer was a procurement agency who was acquiring a system on behalf of the end-user agency, and there were anguished cries from the end users who didn't even recognize the system the bean counters had specified, let alone what we were proposing to provide.

The solution to all the above comes about in engineering change proposals in which the necessary features are finally added at a price which brings the total cost about up to where it should have been bid in the first place.

Bob Hirsch, Sterling Software, NASA Ames Research Center,  
Mail Stop 233-10, Moffett Field, CA 94035 415 694-4807

---

**✉ Re: Lowest-bidder or weak specs? ([RISKS-9.18](#))**

*Bill Cattey <wdc@athena.mit.edu>  
Tue, 29 Aug 89 14:47:58 -0400 (EDT)*

I think David Honig has pointed out a kind of naivety about the process of quality software that allows government and management to persist procurement through lowest bidder.

> It seems to me that if the specifications are complete and correct then  
> there should be no problem.

The problem is that specifications are never complete. The human users and implementors are always finding changes that need to be made. The procurement process must take into account that the spec will evolve over time. The procurement is not only for the product specified, but for the team that builds it, and revises it as it goes along.

> And I cannot think of another decent way to buy systems (the  
> next-to-lowest bidder? the highest bidder?) that will solve the  
problems.

Indeed, this is a hard problem. Here's a suggestion for a procurement process that will do a little more to keep vendors honest:

1. Sealed Bids (same as now)
2. Discard the highest and lowest bids. (Since all bidders are bidding on the same job, if the bids are wildly out of range there's either a problem with the spec or the vendor.)
3. Have those who produced the spec visit the remaining vendors and judge whether the vendor can do what they say they can.
4. Have management choose either the lowest bidder, or the highest quality based on the recommendation made in the previous step.

Any procurement process that reduces to a simple mechanical process engenders RISKS. Although there is the possibility for human error in the process I have suggested, it is designed to address the faults of the existing procurement process of "lowest bidder", while minimizing the risk of doing worse than "lowest bidder".

-wdc

---

### **✂ Pilot simulator training and boredom**

*Dan Franklin <dan@BBN.COM>*

*Wed, 30 Aug 89 22:26:29 EDT*

If, on the one hand, pilots in modern automated planes risk falling asleep from boredom, and on the other hand, they never seem to get enough simulator training in really oddball failures and problems, maybe future cockpits should be designed with simulation software built in, to allow them to practice while they fly.

They couldn't be as good, naturally. Real cockpit simulators simulate everything, including the motions of the simulated airplane, but perhaps going a few rounds with something more modest, along the lines of a video game, would be useful nonetheless. And it would certainly keep the pilot awake! You just need to make sure the simulation is never confused with the real thing...

Dan Franklin

---

### **✂ More on automation**

*Robert Dorsett <rd@rascal.ics.UTEXAS.EDU>*

*Thu, 24 Aug 89 10:34:57 CDT*

>However, the article does not objectively cite balancing situations in which  
>automated systems handled sets of conditions that were too complex and changing  
>too fast for humans ever to respond satisfactorily.

That's probably because such situations don't tend to exist. Automation in airliner cockpits serves to reduce workload, such as when entering congested terminal areas. To insinuate that the pilots \*could never\* handle such situations is to ignore that single-pilot general aviation IFR operations do it all the time. There may be two exceptions to this generalization:

(1) Extending routine automation into critical weather situations, namely 0/0 (Category III) landing. Airliners can now land in weather that most of us wouldn't be caught dead driving in. Think about it...:-)

(2) A secondary layer, usually transparent to the pilot, when his airplane itself is so aerodynamically unstable that he could not hope to control it in a consistent manner over time. In this case, the flight-control system "simulates," in-flight, either traditional (as in the case of the 747, which tries to provide the "feel" of a 707, through control-force dampers or amplifiers) or untraditional (A320/330/340) flying characteristics.

<> Still, while simulator training could help for some kinds of emergencies,  
>One wonders, "Why not?" Can the great minds of the aircraft industry not  
>postulate virtually any kind of emergency?

Writing simulators is extremely difficult. The computational ability may not be available to accomodate higher-fidelity simulations, even if a satisfactory method existed to write the billions of lines of code required to represent \*every\* fault situation. The most cost-effective method, and the current trend, has been to identify those factors which are most likely to occur in a flight (emergency and otherwise), and represent them as realistically as possible. In certain cases, "classic crashes" (such as windshear incidents) may be simulated and pilots run through them.

Rolfe's text, *\_Flight Simulation\_*, is a nice overviews of the problems and promise of flight simulators, both military and civil.

>For years, the US Air Force has been  
>flying high performance tactical jets using significant amounts of automation.  
>If the automated system fails, the game is over.

The automation is an essential component of the flight control system for these types of aircraft. And if it fails, like you say, the game is over: EJECT. That option does not exist in civil situations.

>The entire article is a good example of the warped treatment afforded a  
>complex, scientific topic by the popular press.

The article was largely on-base. If anyone would like to see what other "so-called experts" have to say, I recommend Nagel and Wiener's *\_Human Factors in Aviation\_* (Academic Press: 1988, \$65 or so, hardcover).



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 9: Issue 21

Tuesday 5 September 1989

## Contents

- [Re: Technology doesn't have to be bad](#)  
[Brian Randell](#)
- [Medical systems and RF interference](#)  
[Edward A. Ranzenbach](#)
- [`Business Week' on computers and privacy](#)  
[Rodney Hoffman](#)
- [Law == Ethical Consensus](#)  
[Scott Guthery](#)
- [US occupational hazards much worse than in Europe, report claims](#)  
[Jon Jacky](#)
- [Are on-line pictures RISKy?](#)  
[Russ Nelson](#)
- [Non-U.S. Postal Codes -or- Cheap Mail to Europe](#)  
[Michael Franz](#)
- [Tired of computers being trusted?](#)  
[Hugh Davies](#)
- [Re: lowest-bidder](#)  
[Donald Lindsay](#)  
[Bill Anderson](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **✉ Re: Technology doesn't have to be bad (Don Norman, [RISKS-9.15](#))**

*Brian Randell <[Brian.Randell@newcastle.ac.uk](mailto:Brian.Randell@newcastle.ac.uk)>  
Mon, 4 Sep 89 10:07:32 BST*

I was delighted by Don Norman's piece in [RISKS 9.15](#), since I too feel that RISKS could and should be even better, and I very much liked the illustrative examples he gave of the sorts of discussions that it would be nice to see in RISKS. (Peter Neumann's comment, stating that RISKS by its very nature attracts stories of failures rather than successes is also true, but somewhat misses the point.)

I have in the past tried on occasion to stimulate discussion of general issues,

rather than just of the details of specific incidents, but without much success. Let me try again, on the subject of risk assessment this time, using some points that I made during a panel session at the recent IFIP Working Conference on Dependable Computing Systems for Critical Applications.

Ideally, deployment of any potentially risky computer-based system will be preceded by the sort of careful assessment of the risks involved that is typical in a number of engineering disciplines. There are a number of well-established techniques for such risk assessment, such as Failure Modes and Effects Analysis, Event Tree Analysis, and Fault Tree Analysis. As I understand it, all of these involve enumeration and consideration of possibilities, and identification of dependencies, which are then represented in some sort of graph structure, but none of the ensuing analyses take account of the possibility that this graph structure will be incorrect. To my mind, this makes these techniques of limited value for systems employing computers running large suites of software.

In making this statement, I have three characteristics of such systems in mind: (i) their great logical complexity, and hence the danger of their harbouring potentially risky design faults, (ii) the largely discrete nature of their behaviour, which means that concepts such as "stress", "failure region", "safety factor", which are basic to conventional risk management have little meaning, and (iii) the almost ethereal nature of software, which makes it much more difficult to identify appropriate components and to understand their interactions (both planned and accidental) than with many physical systems.

It is of course good practice to design software with a highly modular structure, and to try to isolate critical parts of the software in as small and simple a subsystem as possible. However with a really complex system such structuring is again essentially ethereal and by no means simple. There will therefore remain a significant and unquantifiable likelihood that such modularisation and isolation is itself faulty.

I thus believe that the graph structure which purports to represent, at any significant level of detail, the internals of (especially the software in) a complex computing system, is likely to be wrong, in that it will not represent any residual design faults properly, so that such faults will remain an (unquantified) contributor to overall system risks.

The question of whether we will ever be able either to guarantee that a complex computing system is entirely free of design faults, or alternatively able to quantify the likely impact of residual design faults is moot. The point I am trying to make here is that in present circumstances, I see no current alternative to basing the assessment of the risks of the overall system on a worst case scenario for the behaviour of the computing system, based on the physical capabilities of its interfaces to the outside world, rather than on mere hopes about its internal activities - and to taking appropriate precautions externally to the computing system. Yet, unfortunately, one sees these days the opposite trend: namely the increasing use of computing systems in situations where there is little or no ability of some surrounding system to mask the failures of the computing system.

It would be nice to learn the reactions to the above comments of people who have tried applying conventional risk assessment and management techniques to

systems involving really complex software.

Brian Randell, Computing Laboratory, University of Newcastle upon Tyne  
+44 91 222 7923

---

### **✂ Medical systems and RF interference...**

*"Edward A. Ranzenbach" <Ranzenbach@DOCKMASTER.NCSC.MIL>  
Tue, 5 Sep 89 12:15 EDT*

Last evening I visited a local hospital ICU to check on the status of a patient I had treated and transported earlier in the day (I am a certified paramedic, in my copious spare time). The patient was on a state-of-the-art mechanical respirator. While discussing the patient's case with the attending physician at the patient's bedside, the respirator failed, accompanied by a visual and auditory fanfare of alarms. The physician quickly reset the device and we continued our discussion. Moments later the device once again failed and had to be reset (it should be noted that a number of differing events can cause alarms in these devices and they occasionally need adjusting and service). By the third occurrence of this failure I had noticed a pattern. Each time I heard radio traffic on my portable radio (in the 800 MHz band) the respirator failed. We were not transmitting mind you, only receiving but this seemed to be enough to set off the alarms. Just then we received a call and when my partner keyed his mike to transmit several other respirators in adjoining rooms also became alarmed and prompted a flurry of activity to reset them. Needless to say, our radios are now banned from the unit. Unfortunately, I had to leave abruptly and did not have time to research the model or manufacturer but will follow up when the opportunity presents itself.

Perhaps it is time to require TEMPESTing of medical equipment... -ear

---

### **✂ 'Business Week' on computers and privacy**

*Rodney Hoffman <Hoffman.ElSegundo@Xerox.com>  
1 Sep 89 07:43:52 PDT (Friday)*

'Business Week' magazine for Sept. 4, 1989 features a cover story entitled IS NOTHING PRIVATE? The teaser line says "Computers hold lots of data on you -- and there are few limits on its use"

The article focuses mainly on financial data, especially credit records.

It includes some good sidebar pieces:

- \* THE RIGHT TO PRIVACY: THERE'S MORE LOOPHOLE THAN LAW  
(reviewing existing privacy laws)
  
- \* NEVER MIND YOUR NUMBER -- THEY'VE GOT YOUR NAME  
(guarding your Social Security Number is almost pointless today)
  
- \* THE SCOOP ON SNOOPING: IT'S A CINCH  
(it's easy for almost anyone to get almost anyone else's credit records)

In that last piece, the reporter posed as an employer checking out potential job candidates. He was required to produce almost no verification. He then requested, among other things, the credit record for one Dan Quayle (at an Indiana address taken from an old "Who's Who in the Midwest"). This raised no alarms. It turned up an "a.k.a. J. Danforth Quayle" with a Washington-area address, who charges more at Sears than at Brooks Brothers and has a big mortgage. It gave his credit card numbers, etc. The Vice President's office was not amused. "We find the invasion of privacy aspect of the credit situation disturbing. Further controls should be considered," said a spokesman.

---

### **✂ Law == Ethical Consensus**

*Scott Guthery <guthery@acw.UUCP>  
Mon, 4 Apr 88 08:07:50 CDT*

Donald J. Weinsbank in a recent posting (via Tom Thomson) to RISKS asks if the law is all we can appeal to in teaching ethics. The answer, at least in U.S. taxpayer-supported institutions, must be "Yes". The law *\*IS\** the current ethical consensus. To go beyond the law in a course taught at a taxpayer-supported institution is to begin to mix state and religion which we in America have agreed through law making that we won't do. A teacher in a institution receiving U.S. taxpayer support is legally obliged to state from the front of the classroom that if it isn't illegal it is by definition ethically correct.

---

### **✂ US occupational hazards much worse than in Europe, report claims**

*Jon Jacky <JON@GAFFER.RAD.WASHINGTON.EDU>  
Tue, 5 Sep 1989 12:46:48 PDT*

The following story appeared on the front page of THE SEATTLE TIMES, Monday September 4, 1989:

WORK IN US: HIGH DEATH RATE --- Associated Press and United Press International

... The National Safe Workplace Institute found that more workers are killed on the job in this nation than in most other industrialized countries. ... US workers are 36 times more likely to be killed than a Swede, and nine times more likely to be killed than a Briton, it said. The report said one out of 14 workers will be killed or seriously injured at work. ...

[ Such a big difference is surprising to me. Is this for real? It is often noted that European safety regulations are generally more stringent than those in the US. Does this contribute to the reported difference, or is the effect dominated by some other factor - e.g., proportionately more people employed in hazardous industries in the US?

This report may seem only marginally related to RISKS; at COMPASS '88 last year

someone cited a study that said about two percent of industrial accidents were attributable to control system failures. - JJ]

- Jonathan Jacky, University of Washington

---

### **✂ Are on-line pictures RISKy?**

*Russ Nelson <nelson@sun.soe.clarkson.edu>*

*Fri, 1 Sep 89 22:31:26 EDT*

Does anyone have any experience with the RISks of digitized faces such as are found on uunet.uu.net:/faces? I want to gather digitized faces of our staff members and students to make them publicly available. I would like to be forewarned of any problems that other people have encountered.

--russ (nelson@clutx [.bitnet | .clarkson.edu])|(70441.205@compuserve.com)|  
(Russell.Nelson@f360.n260.z1.fidonet.org)|(BH01@GEnie.com :-)

---

### **✂ Non-U.S. Postal Codes -or- Cheap Mail to Europe**

*<franz@ceres.inf.ethz.ch>*

*05 Sep 89 11:25:59+0200*

Quite regularly I receive mail from sources in the U.S., whose computer systems are obviously unable to handle European-style postal codes (not fitting the two-letter-plus-five-digit scheme).

Coming in the mail today was something new: A mass mailing from a North Californian company, directed at my street address in

Switzerla, ND 08008 (my four-digit Swiss postal code zero extended)

I still wonder, whether the typist who entered my address that way acted out of ignorance or in a flash of genius...

Interesting enough, the U.S. Post Office people in California must have believed that "Switzerla" is somewhere in North Dakota. I don't think that "Bulk Rate U.S. Postage PAID" mailings are usually transported overseas... All other mail of this type that I receive has some extra postage added.

This should be investigated. How about writing a letter to those friends of yours in Germa, New York or those in Brita, Indiana... :-)

Michael Franz, Computersysteme, ETH Zurich, Switzerland +41-1-256'22'23

---

### **✂ Tired of computers being trusted?**

*<"hugh\_davies.WGC1RX"@Xerox.COM>*

31 Aug 89 07:37:35 PDT (Thursday)

Recently, my beloved (and elderly) Porsche 924 Turbo expired at the roadside. It has a electronic engine management system, and after some initial investigation (including discovering that the hardware doesn't match the manual!), I realised that the problem was (a) in the EMS, and (b) beyond my ability to diagnose. I had it towed to the nearest dealer.

After a few days, I rang the dealer to find out what had happened. They said "We can't find out what's wrong with it". I rang back the following day, and the day after - Same story. Then I went there. The service manager sheepishly admitted that their diagnostic computer was faulty, and after several attempts to diagnose my car, they'd tried it on one of the new 944s in the showroom, and it had diagnosed that as faulty. They'd had to return the diagnostic computer to Porsche UK Headquarters for replacement, before they could fault-find my car.

Motto: "Who will diagnose the diagnostics?"

Hugh Davies.

(P.S. Oh yeah, the fault. New EMS, H.T. module and other bits and pieces. \$1600. Sigh.)

---

### **✉ Re: lowest-bidder: use Points**

*<Donald.Lindsay@MATHOM.GANDALF.CS.CMU.EDU>*

*Sun, 3 Sep 1989 00:25-EDT*

The discussion to date has been long on complaints, but short on workable suggestions. I would like to put forward a system which was in use in Canada, back when I freelanced.

Each bid was assigned points. There were points for having been in business a while (stability). There were points for having completed past contracts successfully (competence). There were points for having the necessary employees in hand.

Note, by the way, that bids are not necessarily just dollar values. They may also contain specific plans, which differ in both the proposed method and the proposed result. These can be evaluated, and given merit points. For example, a bidder may have seen a way to reduce costs, or may have argued that a danger to the public safety must be reduced, or whatever. These proposals may try to justify a lower bid, or a higher bid. The proposals might be judged to have low merit, because e.g. the review board wasn't willing to cut costs in the proposed manner, or didn't want to buy that much public safety.

Since this was the government, they could also assign points for "agenda" items: Canadian content, number of jobs created, minority and regional issues, being a small business, development of a useful technology, whatever. I never learned exact details, but then, I am putting this forwards as a workable general idea, not as some sort of precise formula.

For example, it is possible to give security points to computer purchases. Bids proposing MSDOS would lose all of these points. However, if the product didn't require much security, then MSDOS might still be in the winning bid.

Don

---

**✉ Re: Lowest bidders ([RISKS-9.20](#))**

<WAnderson.wbst@Xerox.COM>

5 Sep 89 09:49 EDT

A friend of mine who has his own business has this quote from John Ruskin (the 19th Century English social critic) on his office door:

"It's unwise to pay too much ... but it's worse to pay too little. When you pay too much, you lose a little money ... that is all. When you pay too little, you sometimes lose everything, because the thing you bought was incapable of doing the thing it was bought to do.

The common law of business balance prohibits paying a little and getting a lot. It can't be done. If you deal with the lowest bidder, it is well to add something for the risk you run. And if you do that, you will have enough to pay for something better."

Bill Anderson, Xerox Corp.



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 9: Issue 22

Wednesday 6 September 1989

## Contents

- [Paris computer takes law into its own hands](#)  
[ST4012704 and Sally Jubb](#)
- [Brian Randell's comment on fault/failure analysis](#)  
[Ted Lee](#)
- [Re: US occupational hazards much worse than in Europe](#)  
[Mats Ohrman](#)
- [Re: medical systems and RF interference](#)  
[Brian Kantor](#)
- [Re: mis-tagging](#)  
[Olivier Crepin-Leblond](#)
- [Electronic House Arrest Failure](#)  
[Martyn Thomas](#)
- [Re: Lowest-bidder or weak specs?](#)  
[Henry Spencer](#)
- [Re: Law == Ethical Consensus](#)  
[Douglas W. Jones](#)  
[Victor Yodaiken](#)  
[Gilbert Harman](#)  
[Eric Hughes](#)  
[Bill Murray](#)  
[Joel M. Halpern](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **Paris computer takes law into its own hands**

<ST4012704@PRIME-A.OXFORD-POLY.AC.UK>

Wed, 06 Sep 89 17:34:18 BST

(From "The Guardian" - National Daily Newspaper) Wed 6-Sep-1989

A crusading computer has taken the law into its own hands and caught 41,000 Parisians on charges of murder, extortion, prostitution, drug trafficking and other serious crimes. But the big round-up ended in embarrassment after an admission by the City Hall yesterday that the electronic Batman could not tell

the difference between a parking offence and gang warfare. "The accused persons will be receiving letters of apology." an official at the City Hall Treasury department said. "Instead of receiving summonses on criminal charges, they should have been sent reminders of unpaid motoring fines in April. Somehow or other the standard codes we use for automatically issued reminders got mixed up."

The first hint of the avenging computer's self-appointed mission to clean up the capital came at the weekend. Hundreds of Parisians received printed letters accusing them of big crimes, but demanding only petty fines for the major crimes of between #50 and #150 (pounds - UK equivalent). "About 41,000 people are involved and some of the charges are quite weird." the official admitted. "One man has complained of being accused of dealing in illegal veterinary products. Unfortunately, other accusations went much further, like man-slaughter through the administration of dangerous drugs." "There were a lot of cases of living off immoral earnings, racketeering and murder." The official said an inquiry had been started to see if the caped computer had a human accomplice. So far, no one has asked the Joker if he was in Paris last week.

[Also noted by Sally Jubb <salj@hplb.hpl.hp.com> ]

---

### ✂ Brian Randell's comment on fault/failure analysis ([RISKS-9.21](#))

<TMPLee.TIS@DOCKMASTER.NCSC.MIL>

Tue, 5 Sep 89 21:05 EDT

I'd like to add one postscript to Brian Randell's observations about the difficulty (impossibility? perhaps) of analyzing the failure modes and latent defects of complex computer systems. Fault tree analysis, etc., may well be valid and useful if all one is doing is estimating the probability of failure under "normal" (even if stressed to the extreme by incompetent operators or "acts of God") operation. One must note, however, that if the system is being "stressed" by a conscious, knowledgeable, determined, perhaps well-funded, "enemy" even his pessimistic analysis is too-optimistic: if the system has exploitable flaws they WILL be found; it's only a question of time and energy.

---

### ✂ Re: US occupational hazards much worse than in Europe, report claims

Mats Ohrman <matoh@sssab.se>

Wed, 6 Sep 89 08:14:23 GMT

JON@GAFFER.RAD.WASHINGTON.EDU (Jon Jacky) writes:

>... The National Safe Workplace Institute found that more workers are  
>killed on the job in this nation than in most other industrialized  
>countries. ... US workers are 36 times more likely to be killed than  
>a Swede,

>[ Such a big difference is surprising to me. Is this for real? It  
>is often noted that European safety regulations are generally more

>stringent than those in the US.

Doesn't surprise me. Swedish safety regulations are VERY strict.

\*Any\* place with more than five employees has to have a safety ombudsman, an employee trained to recognize hazardous situation, who has the authority to stop any work that seems dangerous. Death accidents at work (other than traffic accidents) are rare enough to usually make it into the national media (and draw rather large headlines).

On the other hand, there are people comparing living in Sweden to living in a padded cell. Oh, well...

—  
Mats Ohrman

Scandinavian System Support AB, Box 535, S-581 06 Linköping, Sweden

---

**✉ Re: medical systems and RF interference (Ranzenbach, [RISKS-9.21](#))**

*Brian Kantor <brian@ucsd.edu>*

*Tue, 5 Sep 89 21:24:24 -0700*

If your radio was part of an 800MHz "trunked" radio system, it may have transmitted even when you were not keying the microphone.

Trunked radio systems work by sharing a pool of channels between many users. When a user transmits, he briefly interrogates the controller and is temporarily assigned one of the pool of channels for his use. After some idle time, the channel is considered available for use by other members of the trunked system. Normally each mobile (which includes portables, etc) is monitoring a "home" channel, but when any unit in the system transmits, the repeater controller sends a signal out that directs ALL the units of that customer to switch to the channel chosen, typically for the duration of the dispatch. The mobiles normally do NOT acknowledge this switching, so they don't transmit for that reason. In this way they differ from a cellular telephone.

However, it is possible to equip mobiles with unit status reporting that allows the base or repeater to poll each unit for its current status and can even be used (in wide-area multiple-receiver trunked systems) to guess a rough location of the unit. If your system were equipped with such an option, it might well cause your walkie to key up even if you aren't talking on it.

There are, of course, other reasons for radios to key inadvertently. I recall a prime example when the local fire department kept getting jammed; it turns out that water from the fire hoses was spraying into a gap in the external-microphone plug in their walkies and keying the transmitter. Of course it only happened when they needed a clear channel most: at a working fire.

However, NO piece of life-support equipment should be as RF sensitive as you describe that respirator to be. There is simply too much RF in the world around us to allow that kind of shoddy design.

- Brian

---

**✂ Re: mis-tagging**

*Olivier Crepin-Leblond <ZDEE699@elm.cc.kcl.ac.uk>*

*Fri, 1 SEP 89 14:35:29 GMT*

The UK experiment with electronic tagging does apply ONLY to remand prisoners who are not necessarily 'criminals' in the sense of killing/attempting to kill someone. I referred to them as criminals, since in the English language, you can call any breach of the law a crime. Speeding on the highway is a 'crime'. Anything which is punishable by law can be put under a general heading of 'crime'. However don't take my word for this since I am French, so I am sure that other people are more qualified than me to decide about this. I thank Geraint Jones for pointing this out. I just didn't think people would get confused about this.

Olivier Crepin-Leblond, Electrical & Electronic Eng,  
Comp. Sys. & Elec., King's College London, UK.

---

**✂ Electronic House Arrest Failure**

*Martyn Thomas <mct@praxis.UUCP>*

*Mon, 4 Sep 89 12:15:53 BST*

A recent RISKS reported the experiment with electronic "tagging" of a suspect awaiting trial in the UK. The system seemingly involves a transponder permanently attached to the suspect's leg, interrogated at random by a transmitter attached to a phone. If the transponder fails to respond, the police are alerted that the suspect may have "escaped".

Datalink newspaper (September 4th) reports that "the only person to have been tagged [ ... ] was woken in the early hours last week when a fault in the [ ... ] system keeping tabs on him alerted the police to an 'escape'."

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK.

---

**✂ Re: Lowest-bidder or weak specs? ([RISKS-9.18](#))**

*<henry@utzoo.UUCP>*

*Tue, 5 Sep 89 23:11:36 -0400*

>2. Discard the highest and lowest bids. (Since all bidders are bidding  
>on the same job, if the bids are wildly out of range there's either a  
>problem with the spec or the vendor.)

Unfortunately, discarding the low bid \*sometimes\* disqualifies precisely the people who are best suited to do the job: the ones who have found a new approach that radically simplifies the problem. The Douglas proposal for what became the A-4 Skyhawk (1950s carrier-based light bomber) specified half the weight -- and half the price -- that everybody else thought reasonable. In the beginning, everyone thought Ed Heinemann (the chief

designer at Douglas) was either crazy or trying to pull a scam. The Skyhawk arrived on schedule, on spec, on budget, on price, and on weight, and was built by the thousands in an enormously successful program.

If the bids are wildly out of range, it may be because somebody's got more than usual insight into what's going on. This might be either a realistic assessment of the real cost of the project, leading to a high bid, or a new approach, leading to a low bid. Either way, accepting the out-of-line bid could be the right thing to do. Unfortunately, it's really hard to tell for sure. You can't just look for some radical difference in the proposals, because there may not be one. Heinemann didn't coat the Skyhawk with antigravity paint; he was just unusually firm and thorough about finding ways to reduce weight.

Henry Spencer at U of Toronto Zoology  
uunet!attcan!utzoo!henry henry@zoo.toronto.edu

---

### **✉ Re: Law == Ethical Consensus**

*Douglas W. Jones <jones@pyrite.cs.uiowa.edu>  
Wed, 6 Sep 89 09:31:16 CDT*

I must take issue with Scott Guthery's piece in [RISKS DIGEST 9.21](#), dated 4 Apr 88 (no doubt, due to unusual congestion somewhere in UUCP).

He says that

> The law *\*IS\** the current ethical consensus.

I will not argue that point, leaving that issue to those more versed in both the law and ethics.

He goes on to conclude that

> A teacher in a institution receiving U.S. taxpayer support is legally  
> obliged to state from the front of the classroom that if it isn't illegal  
> it is by definition ethically correct.

This is nonsense.

I am an associate professor at the University of Iowa, supported totally by tax dollars. Like most publically supported universities, we teach courses on ethics and on religion, and even in our computer science classes, we occasionally discuss ethical issues that are not addressed by the law. Although the public school systems of our country have seemed to have an incredibly difficult time with doing this, the universities have always done it. The key do doing so is fairly obvious.

The University of Iowa College of Liberal Arts Classroom Manual (1983) governs the conduct of classes in my college. It states

> No limitation is placed upon the teacher's freedom of expression in the  
> exposition of the teacher's own subject in the classroom or in statements  
> made outside the classroom, so long as these statements are in good taste.  
> However, members of the faculty are morally bound not to take advantage of  
> their positions by introducing into the classroom provocative discussions  
> of irrelevant subjects that are clearly not within their respective fields  
> of study.

Note that we are not bound by any written contract to obey these rules, nor are these rules legislatively sanctioned. These rules do not represent the "moral consensus" of the state. Rather, they represent the "moral consensus" of the college. In a sense, the faculty of the college have imposed this rule on themselves in order to avoid situations that might force the state to reach it's own "moral consensus", codified in law, that might limit our freedom to teach.

If I were to follow the logic Scott Guthery proposes, the fact that the state has taken no legislative stand on what I can teach would imply that it is completely moral for me to teach anything I want.

It is pretty obvious that the statement in our classroom manual is not really restrictive enough, especially for those teaching in the departments of religion, economics, political science, and philosophy. In those departments, our code would suggest that faculty members would be entitled to advocate or even require adherence to particular religious, economic, political and philosophical stands, but doing so is clearly dangerous because it could bring a legislative reaction. Faculty members in those departments almost always have personal stands on such issues, and they are allowed to make their personal views clear, but at the same time, they are expected to tolerate students who disagree with their personal views and not try to impose those views.

Fortunately, we have ethical traditions (most of which are not written into law) which allow us to retain our freedom of expression. It might almost be appropriate to state the following rule as an alternative to Guthery's statement:

Laws are enacted when people fail to adhere to reasonable self-imposed ethical standards.

Peer groups (friends, neighbors, fellow professionals) can all act to reinforce such standards. For example, we have an ethical consensus that stealing is bad, but no laws would have been enacted if it hadn't been for the fact that, despite this consensus, some people steal. In the professions, we have the opportunity to promulgate ethical codes, and in most mature professions, we can impose these codes on ourselves, providing methods to discipline our peers who fail to adhere to these codes. The more we succeed in our efforts at regulating our own behavior, the less need there is for society as a whole to reach a "moral consensus" about how we should have behaved, and encode this consensus in law.

Douglas W. Jones, Associate Professor of Computer Science, The University of Iowa

[I first thought the date might have been a belated April Fool's gag. I suspect I stripped away some of the preceding header that would have indicated a REMAILing of an old item that had not previously appeared in RISKS. Recycling hits high gear? PGN]

---

**✂ Re: Law == Ethical Consensus ([RISKS-9.21](#))**

victor yodaiken <yodaiken%freal@cs.umass.edu>  
Tue, 5 Sep 89 21:07:04 EDT

Scott Guthery writes in [RISKS 9.21](#) :  
>A teacher in a institution  
>receiving U.S. taxpayer support is legally obliged to state from the  
>front of the classroom that if it isn't illegal it is by definition  
>ethically correct.

This is false, and ethically incorrect.

---

**✂ Re: Law == Ethical Consensus ([RISKS-9.21](#))**

Gilbert Harman <ghh@clarity.princeton.edu>  
5 Sep 89 23:36:47 GMT

Scott Guthery [...] is confused. (1) The law *\*IS NOT\** the current ethical consensus. (2) The current ethical consensus, if there were one, is not the same thing as what is ethically correct. (3) What is ethically correct is distinct from what is required by one or another religion. (4) A teacher in an institution receiving U.S. taxpayer support who says that, "if it isn't illegal it is by definition ethically correct" should be dismissed for incompetence both in ethics and in knowledge of definitions.

Gilbert Harman, Princeton University Cognitive Science Laboratory  
221 Nassau Street, Princeton, NJ 08542 HARMAN@PUCC.BITNET

---

**✂ Re: Law == Ethical Consensus ([RISKS-9.21](#))**

<hughes@bosco.Berkeley.EDU>  
Tue, 5 Sep 89 17:21:13 PDT

Religion is not the only other source of ethics in the world. Philosophy, the largest such source, is not the same as religion nor is it the same as the law. Do not blur the distinction between ethics and morals.

The ethics as found in the law should be the \_minimum\_ required.

Eric Hughes hughes@math.berkeley.edu ucbvax!math!hughes

---

**✂ Law, religion and ethical norms**

<WHMurray.Catwalk@DOCKMASTER.NCSC.MIL>  
Tue, 5 Sep 89 21:43 EDT

It is said that in Soviet Russia everthing that is not explicitly permitted is implicitly restricted. Mr. Guthery suggests that in the U.S. everything that is not illegal is implicitly permitted. He seems to feel, indeed claims to know, that in public institutions to claim otherwise is to violate the constitutional ban on state recognition of religion.

Of course, the implication is that law and religion are the only sources of ethical and moral norms. If the source is not law, then it must be religion. For the state to espouse such a norm is to recognize religion.

If indeed state institutions are behaving this way, it would explain a great deal. It would explain viruses, drug abuse, a quarter of a million teen pregnancies, and a million abortions. It would explain 200,000 deaths per year from the use of tobacco, and 20,000 deaths a year from driving under the influence of alcohol.

If state institutions are behaving this way, it would have to fall into the category that Bob Courtney calls "malicious compliance," conforming to the law only when compliance will make the law appear absurd.

Of course, there are other sources for judging right behavior besides law and religion. They include community interest, enlightened self-interest, legitimate national interest, contract, professional ethics or practice, and other concepts of fairness, justice or equity. To that list one can add tradition and religion. However, I confess that when I first created the the list, I forgot tradition and religion; they did not even occur to me until I read Mr. Guthery's posting.

Now, I confess that I erred grievously. I suggest that all those that would suggest that law and religion are the only sources of norms of right conduct, err even more. The position is so absurd, that had I not left religion off my list, equally absurd, I might be tempted to conclude that they were malicious. That is, they took their position in order to demonstrate that the state must recognize an establishment of religion.

William Hugh Murray, Fellow, Information System Security, Ernst & Young  
2000 National City Center Cleveland, Ohio 44114  
21 Locust Avenue, Suite 2D, New Canaan, Connecticut 06840

---

**✉ Re: law == Ethical Consensus**

1606 <jmh@ns.network.com>  
6 Sep 89 15:22:24 GMT

In his article, Scott Guthery states that a Professor at a tax supported institution is required to assert that Law == Ethical behavior.

This is not true, and does not reflect either the law or the ethical guidelines of any of the major professional societies. I agree that the proliferation of non-legal guidelines does not provide a good basis for teaching ethics in computer science. However, the separation of Church and state does not prevent the teaching of a course on Ethical behavior of computer scientists. Nor does it restrict such a course to an explanation of the legal constraints.

(Not that there are Religion departments at most major tax supported institutions. Also, most philosophy departments have several course on ethics, including history and modern thoughts. These courses often deal with the

question of whether certain behaviour is ethical under a certain theory. Often this is reflected against the background of the students and professors natural inclinations and insights into the topic.)

Joel M. Halpern, Network Systems Corporation



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

**Volume 9: Issue 23**

**Tuesday 12 September 1989**

## Contents

- [Risks of RISKS: A bug in sendmail and multiple copies of RISKS-9.22](#)  
[PGN](#)  
[with help from Bill Sommerfeld and Jeff Schiller](#)
- [RF susceptibility of electronics](#)  
[Pete Lucas](#)
- [Some background on the French Farce](#)  
[Dave Horsfall](#)
- [Organizational Accreditation for Computer Assurance: Some Ideas](#)  
[Frank Houston](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✉ Risks of RISKS: A bug in sendmail and multiple copies of [RISKS-9.22](#)

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

*Fri, 8 Sep 1989 14:44:44 PDT*

Some of you were fortunate in receiving just one copy of [RISKS-9.22](#), but the reported record thus far is TWELVE. Apparently the mailing stumbled on a bug in SENDMAIL that gets activated only rarely on LONG lists (but never before for RISKS on the Sun CSL.SRI.COM -- although I had just added a bunch of new addresses before mailing out [RISKS-9.23!](#)).

The RISKS list is LONG despite my continual efforts to consolidate multiple addresses at the same site through redistributions and BBoards, with considerable volunteer help from around the net as well (for which I am enormously grateful -- for example, Ted Tso on behalf of MIT readers and Marc Shannon unwedging the BITNET LISTSERVers have been active far beyond any reasonable expectations). I hope that the few of you who still get private copies can convert to other means of reading RISKS.

Thanks to all of you who reported the multiple mailings, some even observing from the time stamps that the problem had to be at the CSL end. (Surprisingly, nobody asked if I would CATCH 22 before it went any further.) Unfortunately the repetitive mailing started happening late Wednesday afternoon, and we did

not get a chance to kill it until Thursday morning when SENDMAIL was still merrily trying to send out even MORE copies! Sorry.

Yes, this is just another risk of running RISKS. (Some of you may remember a few years ago getting two or three copies of one issue due to a system crash in the middle of processing the list.) But for this one there may be some help.

The following message from Bill Sommerfeld was very helpful.

Date: Thu, 7 Sep 89 00:10:57 -0400  
From: Bill Sommerfeld <wesommer@ATHENA.MIT.EDU>  
Subject: Retransmissions of RISKS Forum noticed

I noticed that we got several copies (nine, as of last count) of Risks 9.22 at Bloom Beacon today.

There is a bug in sendmail that causes it to dump core (with a longjmp botch) in the middle of processing long mailing lists, with the result that the addresses earlier in the list tend to get multiple copies. Bill

[Bill enclosed a patch, which I omit, that was due to Jeff Schiller of MIT Telecommunications. I thought SENDMAIL users might be interested, but did not want to bother everyone with the code. However, Jeff's comments in the code should be quite interesting to you all as an example of a subtle timing problem. Many thanks to Bill (and Jeff)... PGN]

```
** JIS: We change the global variable ReadTimeout to be 5
** minutes. This variable is used by the lowlevel routine
** sfgets to determine how long to wait for input.
** when we get our greeting we return ReadTimeout to its
** previous state. IMPORTANT: The older code I replaced
** used a separate timeout (via a setjmp and longjmp)
** this LOSES REAL BIG if the 5 minute timeout goes off
** for then sfgets gets its stack unwound and leaves
** a lingering event that will eventually cause a longjmp
** to some ancient stack history, sendmail then dies horribly.
** This usually happens only when dealing with large mailing
** lists ("xpert" in this case > 200 recipients), which is
** the LAST place you want to dump core, for then the queue
** files are out of date and LOTS of people get a duplicate
** copy of the message that was in progress.
```

[We were ready to do a major upgrade on SENDMAIL anyway, so I held off on distributing this message awaiting the inclusion of the fix. But in the process of trying to rebuild our SENDMAIL, a NEW old bug was found, so I am sending [RISKS-9.23](#) to get this news to you -- albeit with some trepidation, and with the mailing list split in twain. I hope no one gets run over by the twain. PGN]

---

## RF susceptibility of electronics

"Pete Lucas - NERC Computer Services U.K." <PJML@ibma.nerc-wallingford.ac.uk>

Thu, 07 Sep 89 10:53:51 BST

Medical electronics not RF-proof - doesn't surprise me one bit. It's not just the medical electronics that get troubled this way. There was a case some years back where the fire alarms of a large London hospital were triggered by low level RF (from walkie-talkie radios operating at about 440 to 470MHz - the Police band). A policeman standing in the hospital foyer could easily trigger the alarms if he used his radio. The threat to life of an 'accidental' triggering of fire alarms and the disturbance to treatments consequent on patient evacuation is just as great as direct perturbation of the medical equipment itself.

Manufacturers of electronic equipment just don't realise how RF-hostile the world is. I can crash my IBM PS/2 by operating a 5-watt handheld UHF radio in the same room.

--Pete--

---

### ✦ Some background on the French Farce

Dave Horsfall <dave@stcns3.stc.oz.au>

Tue, 12 Sep 89 13:04:25 est

On the off chance that no-one else has provided this, I came across some background information on the infamous French Farce. Here are some extracts from "The Australian", Tue Sep 12, 1989:

The ministry said the mixup occurred because a central computer misread magnetic bands on some 41,000 files [ mag stripes? ].  
... the amount of the fines was not affected by the mishap, meaning that speeding tickets were transformed into pimping offences but carried only a F360 fine.

Motorists ticketed for failing to stop at a red light were fined for "importing unauthorised veterinary medications", while those whose only offence was crossing a solid white line on the road were charged with "night fishing in a place reserved for fish breeding".

[May the Farce be With You! PGN]

---

### ✦ Organizational Accreditation for Computer Assurance: Some Ideas

Frank Houston <houston@itd.nrl.navy.mil>

Tue, 12 Sep 89 13:49:45 -0400

Some food for thought. Some decades ago hospitals and the medical professions suffered credibility problems both within the health care industry and with the public. The industry attempted to solve these problems through the process of accreditation, which has so far proved fairly successful. I suggest that this model could be effective for software development. Rather than just prescribing development protocols or requiring exhaustive testing, or certified

practitioners, or relying on product history, why not combine these into a comprehensive evaluation? The results could establish a basis for confidence that an organization produces quality software.

Some preliminary thoughts on the model:

#### ACCREDITATION MODEL

##### GOAL

TO REDUCE THE INCIDENCE OF SAFETY, SECURITY, AND  
"RELIABILITY" PROBLEMS IN CRITICAL COMPUTER PROGRAMS.

##### INITIAL SUGGESTED ITEMS FOR EVALUATION

1. Credentials (of personnel and management: e.g., education, experience, PROFESSIONAL CERTIFICATION, etc.)
2. Process (of software development, a la SEI evaluation questionnaire)
3. Product (independent evaluation and test of)
4. Performance (safety and reliability records on released products)

##### ADVANTAGES

Multidimensional evaluation factors (four to start) avoids the "single scoreboard" syndrome of maximizing the quantity being measured regardless of its relevance to performance.

Criteria are not entirely orthogonal, therefore each criterion provides a safety net to catch problems that one or more of the other criteria might miss.

Acquiring a significant body of data, a statistical basis for correlating performance with the other criteria.

Flexible evaluation criteria and flexible standards to allow for continual improvement.

Establishing a historical reference for measuring progress toward the goal, to reduce the incidence of ...

##### DISADVANTAGES

Requires significant investment of time and effort to establish credibility.

Requires cooperation from major customers.

Requires a substantial corps of volunteer firms that are willing to fund the accreditation process by paying substantial

dues to the accrediting organization.

Requires that dues paying members be committed to the accreditation process, that is, be willing to accept negative outcomes and strive to achieve the standards set by the accrediting organization.

## EPILOGUE

Such a model has worked for hospitals and health care organizations, the Joint Commission on Accreditation of Health-Care Organizations (JCAHO, formerly JCAH). The Joint Commission at one time was so strong that accreditation was a significant factor in eligibility for Medicare payments.

The College of American Pathologists carries on a similar accreditation for clinical laboratories.

Neither of these examples is perfect, but they do work to the extent that they force their members to focus on important success factors and continually measure and report the quality of their products and services. Thus, the accreditation body obtains a window on the norms of practice and can stimulate improvement where necessary. The ultimate lever for accreditation is the willingness of paying customers, Medicare, to accept accreditation as a sufficient guarantee of quality service.

THE VIEWS EXPRESSED ABOVE ARE MY OWN AND DO NOT IN ANY WAY REFLECT THE POLICIES OF THE FOOD AND DRUG ADMINISTRATION.

Frank Houston, FDA/CDRH



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 9: Issue 24

Thursday 14 September 1989

## Contents

- [RISKS-9.22 and RISKS-9.23 problems had different causes!](#)  
[PGN](#)
- [Risks of RISKS: A bug in sendmail and RISKS-9.22](#)  
[Scott Mueller](#)
- [Phobos 1 & 2 computer failures](#)  
[Ralph Hartley](#)
- [Aircraft simulators](#)  
[Rob Boudrie](#)
- [Speeders' Delight?](#)  
[Anthony Stone](#)
- [Medical accreditation: based on "customer" clout?](#)  
[Bob Ayers](#)
- [RISKS in mainstream entertainment \(Mission Impossible\)](#)  
[Benjamin Ellsworth](#)
- [Software Safety Standards](#)  
[Anthony J Zawilski](#)
- [12th National Computer Security Conference](#)  
[Jack Holleran](#)
- [Info on RISKS \(comp.risks\)](#)

---

### [RISKS-9.22](#) and [RISKS-9.23](#) problems had different causes!

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

Wed, 13 Sep 1989 10:23:37 PDT

My sincere regrets for the annoyance to you (and to me receiving triple the BARFMAIL) for the multiple mailing of [RISKS-9.23](#) -- especially when that issue contained an explanation for the fact that readers received from ZERO to as many as (at least) 12 copies of [RISKS-9.22](#). The problem this time was NOT the long-list time-out problem, but rather the crash-in-the-middle problem with TWO server crashes, resulting in many of you getting THREE copies. (Strangely, a few of you apparently got MORE!)

Although the first of yesterday's two crashes was accidentally human induced,

the second was intentional, necessary for our wizard to unwedge a serious catastrophe that had downed an entire subnet of machines for most of the day. But these were circumstances vastly beyond my control -- which is very annoying for someone who really tries to do things carefully.

There are some strong lessons for RISKS readers. Distributed systems are full of tricky problems (synchronization, timing, distributed atomicity, recovery, fault tolerance, security, etc.) that are very demanding. Furthermore, even if everything were done right in the first place (which is most unlikely), there would still be extreme difficulties in ensuring that such systems would continue to work dependably in the presence of on-line evolutionary development. It is important that computer researchers and developers be subjected to the use of the systems and networks that they develop, under really stressed conditions. Even then there will be lurking problems that are not triggered. So, it is time for some widely used really rugged, secure network software that is hardware-fault tolerant and system-crash-tolerant. For example, SENDMAIL should be resistant to time-outs, system crashes, certain human screwups, debug option attacks, etc. (Maybe such a version already exists?) Overall, you RISKS folks, whose awareness is already heightened, need to play a stronger role in ensuring that R&D is really concerned about stringent requirements.

[End of SoapBox] Peter

P.S. In case you were wondering, I have no intention of making a career of writing notes to RISKS explaining new ways for you to get multiple copies. But I certainly hope this does not recur. [ReCur ==> doggedly persistent ? No, I do not want to be a REcur of havoc. And NO, I am not trying to overflow the mailboxes of private subscribers so that they will cancel their subscriptions.]

---

### **✂ Risks of RISKS: A bug in sendmail and multiple copies of [RISKS-9.22](#)**

*Scott Mueller <scott@ardent.com>*

*Wed, 13 Sep 89 09:05:20 PDT*

Your story of the sendmail bug reminded me of a somewhat similar bug in the UUCP network smart mailer program SMAIL. As nearly as I can tell, if there is an address that needs automatic resolution near the end of an alias file with many (~100) addresses, \*that\* recipient receives one copy of the mailing, but a few of the other recipients in that part of the file get an extra copy. Not nearly as extreme as the sendmail problem, but an irritant nonetheless.

Had you split the RISKS list BEFORE sending out the previous digest, would it have been a 22 twain?

Scott Hazen Mueller, Ardent Customer Support  
(408) 732-0400 x336 uunet!ardent!scott

---

### **✂ Phobos 1 & 2 computer failures**

Ralph Hartley <hartley@aic.nrl.navy.mil>  
14 Sep 1989 08:23:27 EDT (Thu)

>From SCIENCE Vol 245, 8 September 1989 p1045

On 27 March ... the spacecraft was passing near Phobos for what was, by then a routine session of imaging. "It was on automatic operation" he [Kremnev, director of the soviet spacecraft manufacturing plant] said. "To conserve energy, the transmitter was off during imaging. But at the time it was due to restart, no signal was heard on Earth." the control group hurriedly sent up emergency commands," Kremnev said, and they indeed were able to reestablish contact. "They got 17 minutes of telemetry data. But the spacecraft was tumbling so that the only communication was through the spacecraft's small antenna.. Therefore they couldn't decipher the telemetry. Then they lost the telemetry". Phobos 2 was never heard from again.

But since then, said Kremnev, "Considerable time has been taken, and we have been successful in deciphering the telemetry." There is now no doubt that the failure lay in the spacecraft's on board computer, he said, and was not due to, say, a meteoroid collision. "after the failure of Phobos," he said, "People at Babakan said 'We have luck only with women - not spacecraft!'"

Kremnev also offered new details as to how the Phobos 1 spacecraft was lost last year on the way to Mars. As part of the ground checkout prior to launch, he said, the spacecraft computer had been loaded with a program for testing its steering. Once the test was completed, of course, the program was no long[er] needed. However it was in "firmware" - read-only memory - which could only be cleared with special electronics equipment. "We would have had to remove the computer from the spacecraft and take it to the people who could do it," said Kremnev. "[But] we had VERY little time before the voyage. So the program was 'locked in a safe.'" That is, it was sealed off and rendered harmless by other software in the spacecraft computer.

Unfortunately, said Kremnev, "the key was found to unlock the safe." On 29 August 1988, not long after launch, a ground controller omitted a single letter in a series of digital commands sent to the spacecraft. And by malignant bad luck, that omission caused the code to be mistranslated in just such a way as to trigger the test sequence. Phobos 1 went into a tumble that was not noticed until the next attempt at contact, 2 days later. It was never recovered. Kremnev said that future versions will have more on-board safeguards.

And what happened to the controller who made the error? Well Kremnev told SCIENCE with a dour expression, he did not go to jail or to Siberia. In fact, it was he who eventually tracked down the error in the code. Nonetheless, said Kremnev, "he was not able to participate in the later operation of Phobos"

Ralph Hartley

---

### Aircraft simulators

<ROB.B@te-cad.prime.com>  
13 Sep 89 21:39:21 EDT

A previous RISKS posting suggested that aircraft be programmed to simulate various flight conditions for "practice" while in "routine flight", but stressed the importance of not confusing reality and simulation. How about deliberately confusing the two - a pilot in an emergency situation would not know if it was real or simulation, and could therefore be expected to behave in a calm, professional manner without panic. (Sort of like not telling school children if the fire bell is a true alarm or a drill). The computer would record response to simulated emergencies for review and evaluations by the rear echelon boys.

There is also a vast untapped market for an "aircraft passenger simulator". (get come cramped seats, small rest rooms, hard to view movies and poor food for a few hours). The market would be large, and there are many more aircraft passengers than there are pilots.

Rob Boudrie

---

### ✂ Speeders' Delight?

Anthony Stone <stone@nbc1.GE.COM>

Thu, 14 Sep 89 14:01:31 EDT

Digital Speed Limit Signs Malfunction, Set 75 mph Pace on New Jersey Turnpike

NEWARK, N.J. (AP) - New Jersey native Bruce Springsteen's fabled muscle cars might have a field day on the state's turnpike these days, where digital speed limit signs are mistakenly sanctioning speeds of 75 mph.

State police and turnpike authority officials said the erroneous speed limit has been showing up on about half a dozen of the signs in northern New Jersey because of a computer programming error. The legal limit is 55 mph.

Gordon Hector, a spokesman for the authority, says technicians were trying to correct the problem. He said workers have also been correcting the signs manually while technicians ponder the trouble. Meanwhile, some motorists found the problem amusing.

"It was kind of strange to see everybody below the speed limit for a change," joked Casey Raskob, a Springfield, N.J. attorney. A state police spokesman, who asked not to be identified, said no traffic problems were reported as result. "But I don't think any judge is gonna buy that excuse," he said.

---

### ✂ Medical accreditation: based on "customer" clout?

Bob Ayers <ayers@src.dec.com>

Wed, 13 Sep 89 10:46:37 PDT

In [RISKS 9.23](#), Frank Houston, discussing the accreditation of professionals, writes:

The ultimate lever for accreditation [in the medical domain] is the

willingness of paying customers, Medicare, to accept accreditation as a sufficient guarantee of quality service.

I suggest that this is an understatement. A stronger phrasing would be

The ultimate lever for accreditation is the action of government in defining non-accreditation as proof of the absence of quality, and, ultimately, banning non-accredited service on that basis.

That's the way it works in U.S. medicine.

First, it's not that Medicare accepts accreditation as quality-proof, but will accept real proof too -- rather they accept (as I understand it) only accreditation.

Second, there's the crime of "practicing medicine without a license."

---

### **✂ RISKS in mainstream entertainment (Mission Impossible)**

*Benjamin Ellsworth <ben@hpcvlx.cv.hp.com>*

*Wed, 13 Sep 89 17:05:14 pdt*

I was kind of watching Mission Impossible the other night (the episode had something to do with a "man of 1000" disguises trying to frame the gray haired guy). For some reason the MI team wanted to access to the personnel records of a facility (a prison?). The electronic/computer penetration whiz (the black fellow) says "Unfortunately, they're not on a computer system so I can't break into the records [or words to that effect]." The MI team go on to get the records in a more mundane way (impersonation, breaking and entering, etc).

I was pleased to note the general effect of stating that computerized record keeping was a security risk especially with regards to penetration from outside the physical facility. This mention of "computer fallibility" is a positive change in the entertainment industry.

This message will self-destruct in five minutes.... ;-)

Benjamin Ellsworth, Hewlett-Packard Company All relevant disclaimers apply.

---

### **✂ Software Safety Standards**

*Zawilski, Anthony J <m16143@mwvm.mitre.org>*

*Friday, 8 Sep 1989 13:51:29 EST*

Working Group for IEEE Software Safety Standard

Organizational Meeting

October 2 & 3, 1989; McLean, Virginia

(703) 883 5631 or (703) 883 6086

+++++

This is the first meeting of the working group. We will form working committees and identify major subareas for an IEEE

draft standard on software safety. Dr. Nancy Levenson will present a background briefing. You are encouraged to attend if you want to be a working member of the standards drafting group. Please post this message and forward as appropriate.

\*

\*

Details as to times, locations, local hotel arrangements, and a written agenda may be obtained from:

Cynthia Wright, SSWG Chair at (703) 883 5631

CWRIGHT@MDF.MITRE.ORG or

Tony Zawilski, SSWG Vice Chair at (703) 883 6086

M16143@MWVM.MITRE.ORG

---

## **12th National Computer Security Conference**

Jack Holleran <Holleran@DOCKMASTER.NCSC.MIL>

Wed, 13 Sep 89 15:34 EDT

Dates: October 10-13, 1989

Place: Baltimore Convention Center

Registration: 12th National Computer Security Conference

c/o Office of the Comptroller

National Institute of Standards and Technology

A807, Administration Building

Gaithersburg, MD 20899

Payment: \$150.00 before September 25, 1989, \$175.00 after September 25, 1989

Conference hotels in area, single cost, and local phone numbers:

Hyatt Regency \$99.00 (301) 528-1234

Days Inn Inner Harbor \$59.00 (301) 576-1000

Holiday Inn \$69.00 (301) 685-3500

Baltimore Marriott \$79.00 (301) 962-0202

Radisson Plaza \$80.00 (301) 539-8400

Best Western Hallmark \$52.00 (301) 539-1188

Additional information: Tammie Grice (301) 975-2775

Payment: Mastercard, VISA, checks, money orders, training or purchase requests. (payment to "National Institute of Standards and Technology/Computer Security Conference")



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 9: Issue 25

Friday 15 September 1989

## Contents

- [Risks of distributed systems](#)  
[Eugene Miya](#)
- [Medical accreditation: good for big shops only?](#)  
[Douglas W. Jones](#)
- [The role of government regulation](#)  
[Douglas W. Jones](#)
- [Is modern software design contributing to societal stupidity?](#)  
[Tom Comeau](#)
- [Re: Aircraft simulators](#)  
[Alan J Rosenthal](#)  
[Robert Dorsett](#)
- [Mission: Impossible](#)  
[Robert Dorsett](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **✉ Risks of distributed systems**

*Eugene Miya <[eugene@eos.arc.nasa.gov](mailto:eugene@eos.arc.nasa.gov)>*

*Thu, 14 Sep 89 19:14:35 PDT*

Peter on his soap box notes the "tricky" problems of distributed systems. Anita Jones in her March 1982 survey of multiprocessors in Computing Surveys noted that programming parallel (or distributed) processors as in the Cm\* system was no more difficult than other programming. This has been challenged by other authors (numerous), BUT the software engineering community has by and large ignored issues which might be "unique" to distributed and parallel systems. The education of most students does not include distributed systems, there being a) no standard product lines, all home grown in different ways from standard components, and b) no consistent standard software (despite rough standardization on protocols). One does not buy a distributed system as one buys a computer system (although there aren't many differences); one builds from "scratch." People do not address issues such as synchronization, atomicity, security, etc. in software design classes, these are issues for the "operating systems" class. And it isn't the researchers and developers of

distributed systems who need exposure, we have plenty, it's the students who need this (as if there really were much of a distinction 8).

In short, I believe programming is going to get harder before it gets easier. I believe this, because I am grappling with these issues NOW. I only have to move my mouse cursor into the appropriate window on my workstation to one of my parallel processors.

--eugene miya

---

### ✂ Medical accreditation: good for big shops only?

*Douglas W. Jones <jones@pyrite.cs.uiowa.edu>*

*Fri, 15 Sep 89 08:51:05 CDT*

In [RISKS 9.23](#), Frank Houston suggests that software shops use an accreditation system modelled on that used by hospitals. The suggestion is interesting, but there are some big differences between hospitals and software shops.

One primary difference, from the accreditation point of view, is that most hospitals are big, while many quite competent software shops are small. Hospitals with fewer than 100 employees are rare, while there are many corporations in both the software and hardware fields that are smaller. Many of these corporations are some of the most creative ones in the field, and the development of major ideas in both hardware and software can be credited to them. The administrative overhead of seeking and maintaining accreditation may be easy to adsorb into a large organization, but it is likely to be prohibitive for such small organizations.

Another difference is that most hospitals have only a small number of staff physicians. Most physicians practicing in a hospital are not on the staff, but instead, have an associate relationship. The analogous structure in a software shop would be to have the secretaries, machine operators, and a few of the programmers on the payroll, but to have the majority of the programmers working there on a contract basis, paid by the customers (patients) and not by the software shop. I don't know what effect this has on the notion of hospital accreditation versus software shop accreditation, but I have a hard time believing the effect is small.

Finally, a hospital is a clearly defined organizational unit; even if it is part of a hospital chain, the physical and staff boundaries are easy to define. Many software organizations are far harder to circumscribe. Finding accreditable units in a large corporation may be quite difficult, and I doubt that entire corporations (say Ford or Xerox) are appropriate units of accreditation. From three job interviews I did at Xerox in 1980, I can state that some software groups in that company were clearly among the best I've encountered, while others were horribly staffed and poorly managed. I would hope that these different groups would be separately examined for accreditation purposes, but that brings up the problem of size and expense, because the largest group (and by far the poorest, by all my measures) had only 60 programmers.

Douglas Jones, Department of Computer Science, University of Iowa

---

## ✂ The role of government regulation

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

Fri, 15 Sep 89 09:52:32 CDT

Bob Ayers comment in [RISKS 9.24](#) on Frank Houston's accreditation proposal in [RISKS 9.23](#) was representative of a number of previous comments on my own and other programmer certification proposals in earlier RISKS issues. He said:

The ultimate lever for accreditation is the action of government in defining non-accreditation as proof of the absence of quality, and, ultimately, banning non-accredited service on that basis.

Similar comments were made in response to earlier proposals for programmer certification. These comments are reasonably representative of a fairly extreme libertarian view that government regulation of the free market is inherently inept and has a corrupting influence on the quality of services offered by the market. I believe that these comments need to be answered.

When there is one big customer, I will agree that such a customer has unusual clout. Charles Babbage wrote extensively on this, pointing out in his book, *On The Economy of Machinery and Manufactures*, that the theory that the free market is optimal works only if there are both many competing suppliers and many competing customers. The market price will not be the optimal price for goods in the presence of a monopoly among either the buyers or sellers.

Medicare is certainly a large customer for medical services, and it is indeed a government program, but it does not follow that government is the "ultimate lever for accreditation". In most states, the Blue-Cross Blue-Shield insurance organization is a bigger customer than Medicare, and their policies are certainly a bigger lever. It might be argued that such huge insurance conglomerates can be viewed as pseudo-governmental, but they are largely products of the free market at work regulating itself.

Charles Babbage pointed out a second factor that corrupts the free market, the inability of a customer to discern the quality of competing products. Babbage's examples were largely drawn from early 19th century scandals involving milk adulteration, but what he said applies just as well to medical practice, where I, as customer, am ill equipped to judge the quality of medical care I purchase.

Babbage said that, in the presence of quality problems and in the absence of easily discernable indicators of quality, customers will pay prices well above the market price to buy from a vendor in whom they have confidence. In such a situation, both customers and vendors benefit from independent certifying authorities such as, in the classic case of agricultural products, the USDA. With colleges and universities, accreditation arose largely without government involvement, although the US Department of Education now accredits accrediting agencies.

My favorite example of a purely non-governmental regulatory agency is

Underwriters Laboratories. They are a creation of the insurance industry, and they are the primary and oldest regulator of consumer product safety in the US. The insurers involved cover the manufacturers liability in case of lawsuits over faulty products, while others offer fire and casualty insurance to consumers. Both profit from reduced claims when manufacturers submit products for UL certification, and customers buy only UL certified products.

My point is this: When it is in the best interests the buyers and sellers of a product to have a regulated marketplace, the marketplace will be regulated, and government has little to do with it. Of course, in times when governments are big and all powerful, government becomes a natural choice as a regulatory authority, but in the absence of strong government involvement, insurance companies, market cooperatives, and other organizations will emerge to regulate the market.

Government did not invent the Computing Sciences Accreditation Board, and it did not invent the Institute for the Certification of Computing Professionals. Right now, nobody is forced to seek accreditation or certification, but it is not hard to imagine a few court cases establishing the principle of strict liability for losses caused by software failures, and if this happens, I see little hope for avoiding forced adherence to some kind of accreditation or certification standards in the software industry. If government does not force these on us, the insurance industry that emerges to provide malpractice insurance for programmers will do it.

Douglas Jones, Department of Computer Science, Univeristy of Iowa

---

### ✂ Is modern software design contributing to societal stupidity?

*Chairman, Von Neumann Catastrophe Relief Fund <"STSYSC::TCOMEAU"@SCIVAXM.STSCI.EDU>  
Fri, 15 Sep 1989 16:06:07 EDT*

A mentor from early in my career once told me that if we made a system idiot-proof, only an idiot would want to use it. Are modern software systems directed toward that end? Is it really too much to ask for people to read and understand, and even use, documentation? That's the question at the heart of the article which follows.

Tom Comeau, Space Telescope Science Institute | [tcomeau@scivax.stsci.edu](mailto:tcomeau@scivax.stsci.edu)

>From *\_The DEC Professional\_*, September, 1989, p. 160.

John C. Dvorak, "The Stupidity Factor"

....I recently read [an] aricle...about research on the topic of stupidity being done by Jon Miller of the Public Opinion Laboratory at Northern Illinois University. He discovered that 36 percent of the American public believes that boiling radioactive milk will make it safe to drink.

The more we study stupidity, the more we realize that the technological society toward which we're headed must protect itself from its own inability to keep up with things because of its own stupidity. The public will be

overloaded with bad information and will be unable to distinguish hokum from fact.

People involved in the PC revolution aren't any smarter. Like the general public, they suffer from an overall incompetence that stems from lack of initiative, fear of the unknown, and plain old sloth. ...

Watching Microsoft Windows try to turn the corner on its quest for popularity reflects this. As easy as Microsoft Windows is to use, it's still too hard to use. ...

[Discussion of the difficulties in bringing up Microsoft windows, and consumer resistance to the product.]

The attitude seems to be that if the machine booted Windows automatically and if a lot of extra work wasn't needed, people might like it. Currently, it's too much trouble. The biggest fear is that you'll go through a lot of effort only to be disappointed with the results: The package won't work as advertised, or run your favorite program, or it crashes.

The only computer that has overcome this sloth factor is the Macintosh, with its logical interface. Steve Jobs realized that many people don't read. He put the documentation in pamphlet form. Plenty of information was omitted, but who cares? ...

People don't read documentation. This is part of a national trend towards stupidity, because people don't read anything! ...

[Discussion of author's son, who has difficulty reading and following installation instructions for a software game.]

Is he different from anyone else who refuses to read documentation -- the majority of today's users? In the past, it was easy to condemn documentation writers for their mediocre and hard-to-understand prose. But much documentation today is well-organized, simple and easy to follow. Still, nobody reads it. Even sophisticated users -- the ones who used to read documentation -- have joined the forces of the illiterate. They argue that life is too short and that a good program doesn't need documentation.

What do we end up with? The market demands bulletproof software that's extremely intuitive. Can software be so intuitive that it communicates its commands through some nether world of non-verbal signals? We can expect researches to find out. Meanwhile, interface engineers will make a lot of money.

What does the future hold? Windows will have to change drastically to be popular, and soon 50 percent of Americans will believe that boiling radioactive milk makes it safe to drink.

---

### **✉ Re: Aircraft simulators ([RISKS-9.24](#), Rob Boudrie)**

*Alan J Rosenthal <flaps@dgp.toronto.edu>*

*Thu, 14 Sep 89 18:23:29 EDT*

> ... not confusing reality and simulation. How about  
>deliberately confusing the two - a pilot in an emergency situation would  
>not know if it was real or simulation, and could therefore be expected to  
>behave in a calm, professional manner without panic. (Sort of like not  
>telling school children if the fire bell is a true alarm or a drill).

I think this would be a very bad idea. Pilots in emergency situations should indeed behave in a calm, professional manner, but they should not necessarily

behave the same as if it were a practice simulation. I can't give a good example because I don't know anything to speak of about planes, but I certainly can give a fire alarm example.

In a fire situation, you might jump from a second or third-story window, and sprain some muscles badly, or break some bones. In a fire drill, you would never do such a thing. In extreme situations you would say, "and at this point I would jump from the window, possibly breaking my leg." You wouldn't do it.

The trade-offs during practice and emergencies are different, and should be. It's sad that this means that you can't really simulate emergencies fully. Nevertheless, it's *\*true\** that this means that you can't really simulate emergencies fully.

ajr

p.s. when I was in public school, we were always warned about drills. We knew whether fire alarms were real or not.

---

### ✈ Aircraft simulators (Rob Boudrie, [RISKS-9.24](#))

Robert Dorsett <mentat@vondrake.cc.utexas.edu>

Thu, 14 Sep 89 17:44:05 -0500

> [SAME QUOTE AS CITED BY ROSENTHAL]

The successful resolution of emergencies invariably results in the aircraft being landed ASAP, which isn't terribly profitable. An *\*emergency\** continues until the aircraft is stopped and the passengers deplaned.

As for mucking with the readouts to provide "fault-solving" practice, the problems are that (a) if we have a system so sophisticated, why bother with pilot control in the first place; and (b) once pilots learn to distrust an instrument (say, through negative training), accidents can happen (look at the recent British Midlands 737 crash last January--it was partially attributed to pilot reluctance to trust the new Smiths Industries engine vibration indicator, which replaced a device that, on older aircraft, had proved to be quite unreliable.).

>There is also a vast untapped market for an "aircraft passenger simulator".

>(get come cramped seats, small rest rooms, hard to view movies and poor food

>for a few hours). The market would be large, and there are many more aircraft

>passengers than there are pilots.

Before launching an airplane, the large manufacturers do extensive "comfort" studies on real-scale cabin mockups. They have employees (or volunteers) play the part of victims, etc. They've experimented with some pretty wild layouts, covering seat-back TV to evacuation scenarios. By the time the aircraft is ready for a "launch" decision, a mockup is prepared for customer inspection, and entire "flights" are flown, complete with uniformed stewardesses and meal service. I may be wrong on this, but I believe Boeing pioneered the practice.

Robert Dorsett UUCP: ...cs.utexas.edu!rascal.ics.utexas.edu!rdd

---

**✈ Mission: Impossible ([RISKS-9.24](#))**

*Robert Dorsett <mentat@vondrake.cc.utexas.edu>*

*Thu, 14 Sep 89 17:34:21 -0500*

Lest anyone credit Mission: Impossible with advancing the state of computer literacy, here's a review I wrote a few weeks back on rec.arts.movies...

Mission: Impossible looked interesting this evening, so I watched it. My mistake.

Tonight's episode was concerned with computer viruses. It starts up with a US nuclear submarine "under attack" from an emergency buoy they went to investigate. The buoy infected the ship with a "virus," which screwed up all the control systems. The ship was ultimately destroyed when torpedoes (shot to destroy the buoy as a last-ditch measure, no pun intended) blew up in the loading bay--the sub was destroyed.

The IMF (no not the International Monetary Fund) is called in. Phelps strolls up to an F-111, just landed, and chats with the pilot. The pilot says "climb on in!" What does Phelps find, but his CD player! (the CD replaces the tape recorder/envelope used in the old series). The CD player informs him that this nasty A-rab arms dealer is in the market for the virus. He wishes to market it to "clients in the Gulf," so as to disrupt American warships.

This provides an opening. The arms dealer is going to Hong Kong to bid for the virus. They arrange for him to be detained and a surrogate sent in his place. The person doing the dealing is a US admiral, the ex-head of the American-Russian team on "computer virus disarmament," and is an expert on "digital warfare."

Still with me? :-)

Anyway, bidding starts. The IMF gasses the estate where the bidding's being held, right after the admiral explains that he's giving out the virus for free-it's the \*antidote\* that he's offering for sale. Bidding goes up to \$12 mil before everyone passes out. The admiral crushes the 3.5" Sony disk in his hands before passing out. The evaluation of the man on the spot is that "He's destroyed the disk!" Phelps: "We have to go to Plan B."

Plan B involves setting up a sub simulator. In classic IMF style, the admiral is fooled into believing that the collision of two supertankers caused the gas cloud that knocked everyone out (some combination of chemicals, you see :-)). A Russian warship is also taken out, as are various airplanes. One airplane which crashes is a Russian sub-hunter, which the American sub intercepts. One of the crewmen bring a distress buoy on board. "No, you fools! Don't bring that on board!" Anyway, one thing leads to another, the admiral is conveniently fooled, and, at the last minute, as the ship's about to be "destroyed," he enters the "antidote" by hand: he jumps in front of a computer

terminal, types in raw hex at about 150 character per second, and saves the simulator.

IMHO, this show pushed computer literacy standards back to oh, 1950's science fiction standards.

(Incidentally, someone mistakenly concluded that the above "jumping in front of terminal" incident involved a miraculous use of a password... there was no password!)



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 9: Issue 26

Wednesday 20 September 1989

## Contents

- [Hospital problems due to software bug](#)  
[Joe Morris](#)
- [Man-Machine Failure at 1989 World Rowing Championships](#)  
[Geoffrey Knauth](#)
- [Responsibility, Doctors, Military vs Software Developers](#)  
[Leslie DeGross](#)
- [Organizational Accreditation: More Thoughts](#)  
[Frank Houston](#)  
[Jon Jacky](#)
- [An interesting answer to the distributed time problem](#)  
[Roy Smith](#)
- [Re: Risks of distributed systems](#)  
[D. Pardo](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **✂ Hospital problems due to software bug**

*Joe Morris (jcmorris@mitre.arpa) <jcmorris@mitre.mitre.org>  
Wed, 20 Sep 89 09:54:11 EDT*

>From the \_Washington\_Post\_, Wednesday, 20 September, page F-1 (the separate business section), without permission...

#### SICK SOFTWARE CHECKS IN AT 100 HOSPITALS

Programming Error Affects Admissions

About 100 hospitals around the country, including Washington Hospital Center, were forced yesterday to switch from computers to pen and paper for major bookkeeping functions because a software program could not figure out what day it was.

Officials said there was no permanent loss of data or threat to treatment of patients. But the incident, apparently caused by a mistake in programming, demonstrates how institutions are accepting the risk that major disruptions

might occur in the workplace as more and more functions are handed to computers.

The incident affected hospitals that use software and services provided by a Pennsylvania company called Shared Medical Systems Corp. The company stores and processes information for hospitals on its own mainframe computers and provides software that can be used on IBM equipment.

Problems began to appear at numerous hospitals early yesterday morning. As call after call for help arrived at SMS headquarters, technicians there realized a pattern was emerging and advised clients to shut down parts of their computer systems as they searched for the cause.

The problem was traced some hours later to a program that allows hospitals to automate the ordering and reporting of laboratory tests. Due to a fault in the aging software, the machines were unable to accept as valid the date September 19, 1989, and went "into a loop," refusing to work, spokesman A. Scott Holmes said.

By day's end, computer services at about 100 of SMS's 600-700 client hospitals had been disrupted.

One computer specialist described the problem as a "birth defect", an accidental fault put in a program in its early days that later threatened the system's health, in contrast to a "virus," a program that is written with the deliberate purpose of replicating itself and causing disruption.

The incident also underlined how exacting the computer programmer's art can be. To build a system that handles routine tasks of hospital administration, programmers must write thousands of lines of "code," or computer instructions, that are intended to let the machine know what to do in every conceivable circumstance.

At Washington Hospital Center yesterday, nurses used paper forms to admit patients, saving the information for entry when the computer system was restored. Staff members also had to manually request lab tests because the automated system would not work.

Delays caused inconvenience but "patient care was not affected," said Claire Fiore, director of public affairs and marketing for Washington Hospital Center. By about 5 p.m., the hospital's admissions computers were up and running again.

Also hit was Capitol Hill Hospital, which reported minor disruptions. "We were able to function normally," said spokeswoman Lisa Poulter. "It may just take a little longer to order services."

---

### **✶ Man-Machine Failure at 1989 World Rowing Championships**

*Geoffrey Knauth <geoff@sunfs3.UUCP>*

*Tue, 19 Sep 89 10:27:09 EDT*

In the Petite Finals of the 1989 World Rowing Championships in Bled, Yugoslavia, five strokes into the Coxed Fours race the microphone wire came loose from my cox-box (an amplifier and tiny computer). I lay in the bow and coxed the entire race unaware that the speaker in the stern was out. Some of my crew could hear me, some could not, and in the confusion we rowed vacantly, far below our potential. The truth of a loose wire discovered just after the finish, that I had not fastened the connector well enough, and that a year's worth of hard work and good speed had just been wrecked, contained enough pain and horror to burn in my soul forever.

Geoffrey S. Knauth, Camex, Inc., 75 Kneeland St., Boston, MA 02111  
(617) 426-3577                      standard disclaimers

[Risks are certainly pervasive. This problem is not life-or-death or even row-versus-wade, but nevertheless must have had a devastating effect on all those involved -- but particularly the cox. On the other hand, I am surprised that in a sport so close to being natural (apart from computer designed shells) a computer would be permitted on-board. Next we might have on-line sensors monitoring crew heart rates to probe their limits, automated instructions from the computerized coxswain replacement using digitally synthesized voice and ear-phones, and even remote computer guidance from the coach overhead in a helicopter. Technology knows no bounds! PGN]

---

## **✂ Responsibility, Doctors, Military vs Software Developers**

*Leslie DeGroff <DEGROFF@INTELLICORP.COM>  
Mon 18 Sep 89 09:53:56-PST*

A variety of Risks messages have discussed medical risks, military risks and software accreditation. A recent one from Douglas Jones triggers me to present a different perspective on the issues of risks and accreditations. A fundamental feature of the current medical systems including accredited institutions is that Doctors have a very high level of personal responsibility for what happens. It is not the institution on the line, it's Dr. XXX and in most larger institutions there are reviews of any "failure" that the Dr. must answer to peers that understand the issues quickly after such a failure. There are are drawbacks to this system, in many cases Dr's over compensate to this Command responsibility by disregarding or belittling input from patients or nurses with more contact with patients. In the military also there is a somewhat corrupted notion of command responsibility, officers involved in major incidents/accidents are brought to trial with both career and freedom on the line if there have been fatalities. The breakdown in the military system comes in the fact that the line officers are often in catch 22, if they don't use an automated system they are risking their ship and if they do and it is used to attack the wrong targets they are still at risk.

There are two different messages that come out of consideration of the medical and military systems, one that creator/providers be made more personally responsible and two that users themselves bear major responsibility for results. This would have a multiplicative effect on lowering risks, personal responsibility (ownership) of creators tends to drive craftsmanship and quality and usage responsibility tends to slow down the adoption of risk edge

tools.

Les DeGroff (intellicorp support)

---

## **Organizational Accreditation for Computer Assurance: More Thoughts**

*Frank Houston <houston@itd.nrl.navy.mil>*

*Tue, 19 Sep 89 11:30:45 -0400*

In hope of stimulating more thought and discussion, I submit the following responses to comments about my "food for thought" message.

>Date: Fri, 15 Sep 89 08:51:05 CDT

>From: Douglas W. Jones

>Subject: Medical accreditation: good for big shops only?

>...

>One primary difference, from the accreditation point of view, is that most

>hospitals are big, while many quite competent software shops are small.

>Hospitals with fewer than 100 employees are rare, while there are many

>corporations in both the software and hardware fields that are smaller.

I suggest that Dr. Jones look around his home state and the neighboring states. Many hospitals are not large, and university hospitals are exceptionally large compared with hospitals in general. It may be true that hospitals with fewer than 100 employees are rare, but they are held to standards like JCAHO's to receive Medicare and insurance payments. Moreover, JCAHO accredits many other organizations and facilities, such as nursing homes, which are small.

>Another difference is that most hospitals have only a small number of staff

>physicians. Most physicians practicing in a hospital are not on the staff,

>but instead, have an associate relationship.

Good point. It is also true that many software and engineering shops supplement their staff with consultants, which sets up a similar situation. Nevertheless, I believe that JCAHO reviews credentials and records of both staff and associates when considering renewal of accreditation. The task of reviewing staff credentials for an engineering firm should not be any more difficult.

>Finally, a hospital is a clearly defined organizational unit; even if it is

>part of a hospital chain, the physical and staff boundaries are easy to

>define. Many software organizations are far harder to circumscribe. Finding

>accreditable units in a large corporation may be quite difficult, and I doubt

>that entire corporations (say Ford or Xerox) are appropriate units of

>accreditation.

I do not suggest that accreditation will be an easy concept to implement. Consider, however, the impact of a customer requirement that an organization be "accredited for the development of critical software/systems." I am sure that Ford or Xerox would find a way to identify the appropriate units if FAA made accreditation a prerequisite for award of ATC contracts.

>These comments are reasonably representative of a fairly extreme libertarian  
>view that government regulation of the free market is inherently inept and has  
>a corrupting influence on the quality of services offered by the market.

I must point out that my proposal does not specify accreditation by a government agency. In fact, having close up and personal experience with government regulation, I share some facets of the "libertarian view." JCAHO is not a government agency; it is more like an industry consortium; another reason why I suggested it as a preliminary model.

>Government did not invent the Computing Sciences Accreditation Board, and it  
>did not invent the Institute for the Certification of Computing Professionals.  
>Right now, nobody is forced to seek accreditation or certification, but it is  
>not hard to imagine a few court cases establishing the principle of strict  
>liability for losses caused by software failures, and if this happens, I see  
>little hope for avoiding forced adherence to some kind of accreditation or  
>certification standards in the software industry. If government does not  
>force these on us, the insurance industry that emerges to provide malpractice  
>insurance for programmers will do it.

I believe that government would be quite willing to defer to a private sector institution for regulating developers of critical software and systems, as it has in the case of JCAHO for medical practice. Product liability underwriters and other insurers probably would also.

>Date: Wed, 13 Sep 89 10:46:37 PDT  
>From: Bob Ayers  
>Subject: Medical accreditation: based on "customer" clout?  
>...  
>First, it's not that Medicare accepts accreditation as quality-proof, but  
>will accept real proof too -- rather they accept (as I understand it) \_only\_  
>accreditation.

Legally Medicare and, therefore, Medicaid accept JCAHO accreditation in lieu of their own reviews. JCAHO accredited hospitals are "deemed" to be in compliance with most of the Medicare Conditions of Participation for Hospitals.

I suggest that both individuals and organizations need to be accredited. If you look carefully at my outline, I suggest that an accreditation board might examine professional certifications.

Nancy Leveson has argued very persuasively that, paraphrasing, "...someone competent must bear responsibility for software in critical systems ... some sort of professional licensing or certification is needed." I have been skeptical, but now I think that, with the further incentive of accreditation, professional certification could be made to work.

I do not think accreditation is a "silver bullet." It is just as corruptible as any system of standards; however it uses the power of the marketplace to make corruption counterproductive. Both industry and customers would soon mistrust a corrupt accreditation system.

The views expressed above are my own and do not reflect in any way the policies of FDA.

Frank Houston

---

### **✂ Organizational Accreditation (What is BS5750/ISO9001?)**

*Jon Jacky <JON@GAFFER.RAD.WASHINGTON.EDU>*

*Fri, 15 Sep 1989 16:50:58 PDT*

In RISKS 9(23), Frank Houston (houston@itd.nrl.navy.mil) proposed consideration of some kind of organizational accreditation for software quality --- the idea was, the whole organization would be certified, rather than particular people or products.

Does something like this already exist in the UK? Inside the front cover of SOFTWARE ENGINEERING 88, PROCEEDINGS OF THE SECOND IEE/BCS CONFERENCE, there is an ad from a systems house bearing an official-looking seal that says "BSI - REGISTERED FIRM". The ad copy says, "First Systems House to Win BS5750 (now ISO 9001)", without further explanation.

Can any British RISKS readers enlighten us?

- Jon Jacky, University of Washington

---

### **✂ An interesting answer to the distributed time problem**

*Roy Smith <roy%phri@uunet.UU.NET>*

*7 Sep 89 00:05:09 GMT*

Lots of things in lots of places depend on having a consistent time reference distributed to many places. Lots of people have worked out high-tech solutions to the problem. Most of them don't work very well. When's the last time you saw a master clock system that worked? The one in our building certainly doesn't. Well, today, I saw an interesting solution in Mt. Sinai Hospital in New York. Take any of the thousands of closed circuit TVs in the hospital and set it to channel 6 and you get a picture of a clock. And not a digitized, computer generated picture either. Somewhere there is a TV camera pointed at a good old sweep-secondhand analog clock, and that's what you see on channel 6. Sometimes low-tech solutions are the best.

Roy Smith, Public Health Research Inst., 455 First Avenue, New York, NY 10016

---

### **✂ Re: Risks of distributed systems**

*<pardo@june.cs.washington.edu>*

*Sun, 17 Sep 89 12:05:06 PDT*

In [RISKS 9.25](#), Eugene Miya writes (about the special risks of parallel and distributed systems) that "[i]t isn't the researchers ... who need exposure [to parallel/distributed issues], it's the students who need this [...]"

There are a growing number of schools that are using Ada to replace Pascal and Modula-2 in the introductory programming courses. Using Ada gives a standardized mechanism for introducing issues such as exceptions and (concurrent) tasks.

I think that everybody will agree that distributed/parallel is under-represented, under-standardized, and over-risky. There is hope, however.

; -D on ( Is parallel uniprocessor an oxymoron? ) Pardo



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 9: Issue 27

Thursday 21 September 1989

## Contents

- [Re: Brian Randell's commentary on safety analysis](#)  
[Nancy Leveson](#)
- [Re: Risks of Distributed Systems](#)  
[Charles Shub](#)
- [Re: Hospital problems due to software bug](#)  
[Will Martin](#)
- [Mailer Bug moves to MCI?](#)  
[Jerry Durand](#)
- [Loose wires, master clocks and satellites](#)  
[Peter Jones](#)  
[PGN](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **Re: Brian Randell's commentary on safety analysis**

*Nancy Leveson <nancy@ICS.UCI.EDU>*

*Wed, 20 Sep 89 17:54:03 -0700*

In [Risks 9.21](#), Brian Randell asks for the reactions to his comments from people who have tried applying conventional risk assessment and management techniques to systems involving "really complex software." I have had experience applying such techniques to many real systems involving software, although I am not sure what Brian means by his qualification "really complex." My arguments in this forum have always stressed the need to eliminate unnecessary complexity in safety-critical systems, and I usually refuse to be involved in the analysis of overly complex systems until they have been simplified. Brian writes:

>Ideally, deployment of any potentially risky computer-based system will be  
>preceded by the sort of careful assessment of the risks involved that is  
>typical in a number of engineering disciplines. There are a number of  
>well-established techniques for such risk assessment, such as Failure Modes  
>and Effects Analysis, Event Tree Analysis, and Fault Tree Analysis. As I  
>understand it, all of these involve enumeration and consideration of

- >possibilities, and identification of dependencies, which are then
- >represented in some sort of graph structure, but none of the ensuing
- >analyses take account of the possibility that this graph structure will
- >be incorrect. To my mind, this makes these techniques of limited value
- >for systems employing computers running large suites of software.

Any type of analysis can be wrong, whether applied to hardware or software. In some respects, safety analysis applied to software may actually be less prone to error than that applied to hardware. Software represents the logical structure in itself and, therefore, the analysis is performed on the actual thing that is being analyzed. For systems involving hardware and physical devices, abstract models must be formed first on which the analysis is applied. This extra step (building the logical representation of the hardware) adds an additional possibility of introducing error. In my experience, safety analysis on software is no more error-prone than that performed on complex hardware systems. For example, I have found that it is much easier to build correct software fault trees than system fault trees.

It has also been my experience that the system safety analyses and control devices do take into account the possibility of errors in particular analyses and failure of safety protective devices.

By the way, not all risk assessment techniques involve graph structures. Of the three mentioned, FMEA records information in the form of tables and does not include identification of dependencies. Event Tree Analysis is equivalent to reachability analysis in computer science models and does represent reachable states in the form of a tree or graph structure. Fault Tree Analysis uses a tree in a very different way -- the tree is just a convenient notation for representing a boolean expression that records the relationship between states or events. It could easily be replaced (and often is) by formal logic expressions.

- >In making this statement, I have three characteristics of such systems in
- >mind: (i) their great logical complexity, and hence the danger of their
- >harbouring potentially risky design faults, (ii) the largely discrete
- >nature of their behaviour, which means that concepts such as "stress",
- >"failure region", "safety factor", which are basic to conventional risk
- >mangement have little meaning,

As I understand it, safety factors are built into hardware systems because of the possible inaccuracies of calculations on continuous models, the limitations of these models in representing real systems, and the possibility that the basic assumptions of the models are incorrect for the actual physical systems that the models represent.

Because software can be analyzed using discrete mathematics and logic, some of the need for safety factors in the analysis are eliminated. It is, of course, always possible for the underlying assumptions (e.g., that the computer hardware does not experience failures) of software analyses to be violated. Brian is correct that safety margins may not be useful to protect against this. However, run-time checks on basic assumptions (using built-in test, assertions, TMR, etc.) can be used in computer systems to provide the same function as safety margins in continuous systems. Failure regions and safety envelopes are easily applied to software. Furthermore,

many, if not most, of the safety devices used in conventional risk management are applicable to discrete systems.

- >and (iii) the almost ethereal nature of software, which makes it much
- >more difficult to identify appropriate components and to understand their
- >interactions (both planned and accidental) than with many physical systems.

I don't know what is meant by the "ethereal" nature of software here. Floyd, Hoare, and others who have followed them have demonstrated that the formal semantics of software can be specified and that software can be treated as a mathematical object. Admittedly, analysis on semantically complex software is difficult. This is why the argument has been made that the semantic complexity of the software used in safety-critical systems must be limited as long as our analysis techniques are limited. However, I have rarely found that this limitation is not possible, even when the system of which the computer is a component appears quite complex at the system level. (This goes back to my recent discussion with Dave Parnas in Risks).

I think it is a mistake to underestimate the complexity and difficulty of identifying unplanned interactions in physical systems. Perrow's book on "Normal Accidents" argues that such interactions (stemming from complexity and coupling) are inherently not possible to identify and control in complex physical systems, and he provides many examples of accidents that have occurred as a result. Again, given that at least the software can be thought of and analyzed as a model of itself, in the future we may find that it is actually easier to identify and control such interactions in software than in physical systems.

- >It is of course good practice to design software with a highly modular
- >structure, and to try to isolate critical parts of the software in as small
- >and simple a subsystem as possible. However with a really complex system such
- >structuring is again essentially ethereal and by no means simple. There will
- >therefore remain a significant and unquantifiable likelihood that such
- >modularisation and isolation is itself faulty.

Again, I do not understand the use of the word "ethereal" with respect to software structure. Of course, modularization and isolation may be faulty in software. It may also be faulty in hardware. Engineers also use analysis techniques, e.g., Sneak Circuit Analysis, to attempt to identify unplanned interactions in electronic systems. Unfortunately, this type of fault is as unquantifiable for hardware as it is for software.

John Shore in the Sachertorte Algorithm has argued that physical systems often have simpler interfaces because of the inherent difficulty of building complex interfaces in such physical systems versus the simplicity of making complex interfaces in software. But that does not mean that it is not possible for software engineers to exercise discipline in order to control and limit the complexity of the software interfaces to that which we can analyze with some degree of confidence. Modularization, information hiding, and isolation applied to software are essentially the same procedures that are used to control complexity in hardware.

- >I thus believe that the graph structure which purports to represent, at any

- >significant level of detail, the internals of (especially the software in) a
- >complex computing system, is likely to be wrong, in that it will not
- >represent any residual design faults properly, so that such faults will
- >remain an (unquantified) contributor to overall system risks.

I am not sure what Prof. Randell here means by a "graph structure" representing the "internals" of software. For example, a Software Fault Tree represents a boolean expression of events that can lead to a hazardous condition. It does not represent residual design faults (although the process of building the tree may identify some critical ones) or the structure of the software.

I agree that all design faults cannot be identified with high confidence for software. But safety analysis does not require this. In my experience in using software fault tree analysis on real software systems, the most useful aspect of the technique may lie in its ability to identify hazardous states that need to be detected at runtime (perhaps by assertions or acceptance tests) regardless of the actual design faults (or underlying computer hardware faults) that caused them.

I should add that most safety analysis techniques on physical systems are not able to quantify the contribution of residual hardware design faults on system risks either. They basically quantify only risks based on physical failures, not design errors.

- >The question of whether we will ever be able either to guarantee that a complex
  - >computing system is entirely free of design faults, or alternatively able to
  - >quantify the likely impact of residual design faults is moot.
  - >The point I am trying to make here is that in present circumstances, I
  - >see no current alternative to basing the assessment of the risks of the
  - >overall system on a worst case scenario for the behaviour of the computing
  - >system, based on the physical capabilities of its interfaces to the
  - >outside world, rather than on mere hopes about its internal activities - and >to taking appropriate precautions
- externally to the computing system. Yet,
- >unfortunately, one sees these days the opposite trend: namely the increasing
  - > use of computing systems in situations where there is little or no ability
  - >of some surrounding system to mask the failures of the computing system.

I agree with this conclusion. It is something I have preached for a long time, and, in fact, it is exactly this worst case scenario analysis that is involved in the application of safety assessment and management techniques to software and to systems containing computers. For example, it is what I was suggesting in my discussion in Risks with Bev Littlewood about using a probability of "1" for software failure in system fault trees. Unfortunately, it is not sufficient, and "taking appropriate precautions externally to the computing system" often requires the same type of system level safety analysis including the internal design of the software that Brian seems to be arguing above is not possible.

In particular, risk assessment and management techniques for physical systems may be no less error prone than that applied to software. The hardware backup systems that Brian (and I) suggest may themselves fail or contain design faults. This does not mean that they should not be used; it merely means that multiple "levels of defense" (a term common in the nuclear industry) are necessary including both hardware and software safeguards and analysis.

We should not rely entirely on hardware safety devices. Risk assessment and management at the system level that excludes the behavior of the software in the analysis and in the design of the software is incomplete and thus potentially dangerous.

Furthermore, it is not always possible to design physical devices to mask completely or with high confidence the failures and errors of the computing subsystem. One reason this is true is that the software is usually controlling the other components of the overall system, and it is difficult to build physical devices that are able to identify and mask control errors (versus total failures) before a hazardous system state is reached. When it can, this should obviously be done. But what will we do about other very desirable systems (e.g., medical systems that could in themselves save lives) where this is not possible?

---

**✉ Re: Risks of Distributed Systems ([RISKS-9.26](#))**

*Charles Shub <cdash@boulder.Colorado.EDU>  
Wed, 20 Sep 89 12:17:56 MDT*

>... Using Ada gives a standardized mechanism for introducing issues such  
> as exceptions and (concurrent) tasks.

Ah yes, Ada\* has a standardized mechanism for (concurrent) tasks, but Ada\* unfortunately does not have a good (IMHO) model for concurrent activities to communicate. Their rendezvous is as bad as the "remote procedure call" technology. We also need to discuss asynchronous IPC which is done at even fewer places. This message is an example of asynchronous inter process communication. I can guarantee you that i'm doing other things until you respond or acknowledge (or this message gets dropped in a bit bucket somewhere) and neither RPC nor the rendezvous allows that. So please don't tout Ada\* as the cure-all for concurrency. We all know that  
"dod created ada and it was good."

\* Ada (and nuclear annihilation for that matter) are trademarks of the Department of Defense.

---

**✉ Re: Hospital problems due to software bug ([RISKS-9.26](#))**

*Will Martin <wmartin@STL-06SIMA.ARMY.MIL>  
Wed, 20 Sep 89 13:05:16 CDT*

>Due to a fault in the aging software, the machines were unable to accept as  
>valid the date September 19, 1989, ...  
>One computer specialist described the problem as a "birth defect", ...

Just what we need -- more jargon for the media to splash around. "Birth defect" instead of just simple "error" or the traditional "bug".

Does anyone know if this was one of the built-in magic-number date breakdowns that have previously been mentioned on RISKS? That is, the ones where the

system date/time is maintained in a field containing the number of seconds since some arbitrary start-date in the past, and which will fill up and trip back to 0 at some predictable future date (at which time all applications using that OS or system will trash their date processing and mangle any data based on dates... :- ( ).

I was hoping that someone out there has kept track of and will post a note listing those magic dates for various OS's and systems. It will be a useful reference for all of us.

Regards, Will Martin

---

### **✂ Mailer Bug moves to MCI**

<JDurand@cup.portal.com>

Wed, 20-Sep-89 19:02:35 PDT

I received the following notice today from MCI, it sounds like your MAILER bug ([RISKS-9.22](#), 23) is contagious!

Jerry Durand, Durand Interstellar

Date: Wed Sep 20, 1989 6:45 am PDT

From: FAX Help / MCI ID: 369-3746

TO: \* Durand Interstellar / MCI ID: 114-9128

Subject: Multiple Fax Messages

Dear Customer,

According to our records you sent a Fax Dispatch message Tuesday, afternoon September 19, 1989. Due to a temporary software bug in the system, it is possible that MCI Mail attempted to deliver your message numerous times. Therefore, you may receive several message confirmations or cancellation notices.

This problem, which only affected Fax Dispatch has been corrected. MCI Mail has also taken the necessary steps to insure that you are not billed for any extra messages.

We regret any inconvenience this may have caused you, and will do our utmost to avoid a recurrence of this situation.

Sincerely,

MCI Mail Customer Support

---

### **✂ Loose wires, master clocks and satellites**

Peter Jones <MAINT@UQAM.bitnet>

Thu, 21 Sep 89 10:57:17 EDT

Two articles in [RISKS 9.26](#), namely "Man-Machine Failure at 1989 World Rowing

Championships", and "An Interesting Answer to the Distributed Time Problem" reminded me of a certain performance of Beethoven's Ninth Symphony on December 12, 1988, in which I sang in the tenor section offstage in Montreal. The National Film Board of Canada has just released a video documentary about this event, entitled "Satellite Symphony --- One Woman's Dream".

The dream in question was to conduct an orchestra in Montreal, with choirs in San Mateo, Geneva and Moscow. Unfortunately, as the links between these places were via satellite, there were perceptible delays in satellite transmission, making it difficult to get everyone in sync.

One solution tried was to send a cue to the remote choirs ahead of the conductor in Montreal, so that their sound would come back in time with the orchestra. This proved to be unworkable, for the delay required was in terms of milliseconds, and not in terms of beats and fractions thereof. Also the response times of the remote choir conductors and their singers was difficult to assess, and the main conductor might not be at the same tempo from one performance to another.

The solution that was finally adopted was to transmit a recording of the dress rehearsal of the previous evening to the remote choirs, ahead of the live sound. With the aid of an earphone, the conductor in Montreal would hear and follow the same recording, with a delay to compensate for the two-way satellite transmission of her cues and the choirs' singing in response. (I'm glossing over the technicality that number of satellite "hops", hence the delay, was different for each choir.)

So far, we have seen the master-clocking difficulties. What happened on concert night? Yes, a proverbial loose wire. The conductor's earphone malfunctioned, although the choirs heard the recorded sound by satellite! After a 45-second wait, and a fruitless call for assistance (she couldn't get a reply on the defective earphone without leaving the podium, or having someone come out on stage), she decided to start anyway. Radio Canada technicians sent the live sound to the remote choirs. The end result was that the choirs missed their first entry. Fortunately, the Montreal Symphony's choir was on hand backstage in Montreal as a backup, providing the illusion to the audience that the other choirs had indeed come in. The rest of the choirs managed to come in further on, more or less on time. The resulting sound was, as Spock of Star Trek would say, "Fascinating".

Peter Jones    MAINT@UQAM    (514)-987-3542

---

## **✂ Re: Loose wires, master clocks and satellites**

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

*Thu, 21 Sep 1989 13:22:01 PDT*

Following Hollywood hi-tech practice, and minimizing the real-time risks, next time you might try videotaping the orchestral dress rehearsal in Montreal -- with the option of the local backstage chorus being heard only on ear-phones by the conductor and players, and recorded on a separate audio track -- then letting San Mateo, Geneva and Moscow dub their contributions independently (while each watched the videotaped conductor and heard the dress rehearsal

orchestra audio), and finally mixing the whole thing together in a 'live' performance. That way the conductor would not have to rely on ear-phones -- she would be mimicking herself on the tape monitor while the sound of taped choruses and the prerecorded orchestra filled the hall. The Montreal orchestra folks could synch their playing (especially the wind players, who would indeed be lip-synching) to the recording -- or simply fake it altogether! With a little computer processing you could even do real-time resynchronization to compensate for recording machines that were slightly off speed. However, the whole thing seems somewhat silly because the conductor could not influence the performance in progress, which was presumably her original intent. And the results had to be MURKY! With the transmission delays, you cannot really afford to let anyone hear another group anyway unless recorded; because the time delay from 'ictus' (low-point of the beat) to sound attack generally varies with the tempo, and because it is very difficult to anticipate adequately from auditory cues alone, the visual cues are much more important -- even if tape delayed. Furthermore, if there is no live playing or singing except maybe locally, you can afford to run everything tape delayed with variable delays in the pre-mix. (I hope they weren't singing in English, French and Russian! But I am reminded of two high-school bands getting together unrehearsed in 1949 for the Star Spangled Banner, with one playing in Bb, the other in Ab.)

Perhaps I got parODied away. It happens every now and then. But this is really a marvelous real-time synchronization problem, and the risks in pulling it off are considerable. On the other hand, if you lose one chorus completely, probably nobody in the audience would ever know -- except that the Russian accent in German might suddenly disappear.

Freud would have been amused with the aural fixation.

``Freude, Freude, got 'er, 'funken, {as in RundFunk = broadcast}  
Sighed, `umschlungen, millionen!'" {THAT's a lot of singers.}  
Owed to Joy. Schiller.

``... achoired a certain measure of reknown ..." Tom Lehrer.



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 9: Issue 28

Sunday 24 September 1989

## Contents

- [USAir 737-400 crash at LaGuardia](#)  
[PGN](#)
- [Re: Hospital problems due to software bug](#)  
[Steve VanDevender + Amos Shapir](#)
- [Computers, Planning, and Common Sense \(John J.G.\) Mainwaring](#)
- [Synchronizing Clocks](#)  
[Earl Boebert](#)
- [Re: Risks of Distributed Systems](#)  
[Sung Kwon Chung](#)
- [Master clocks, etc.](#)  
[Eddie Caplan](#)
- [ISO 9001 accreditation](#)  
[Martyn Thomas](#)
- [Toxic Spill at the Department of Education \[long\]](#)  
[Joe Pujals](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✂ USAir 737-400 crash at LaGuardia

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

Fri, 22 Sep 1989 16:21:29 PDT

At the very end of an article in the 22 Sep 89 San Francisco Chronicle from the NY Times ("Cause of Accident a Mystery; Probers Can't Find Pilots in USAir Crash") is this:

``Aviation experts said the controls of the 737-400, a modified and modernized version of a plane that has been one of the most reliable in commercial aviation for many years, are unusual in that they are integrated with computers. Instead of pushing a throttle to accelerate, a pilot uses a computer-like keyboard to enter in a set of commands that set the power of the engines on takeoff. It is possible, experts said, that an erroneous set of numbers was entered and that this accounted for the insufficient power on

takeoff."

Earlier in the article was this:

``... the pilot had flown the planes for only two months, and the co-pilot was said to have been in a 737 cockpit for the first time. ... initial reports indicated that the co-pilot was at the controls during the take-off ... the co-pilot told the Port Authority police shortly after the crash that the pilot had been "mumbling" and "acting irrationally" just before takeoff."

[Saturday's and Sunday's papers stated that officials had indicated that a wrong button had been pushed, although Sunday's paper suggested that there might have been mechanical failure as well... The pilot and copilot have been suspended for disappearing afterwards.]

---

**✂ Re: Hospital problems due to software bug ([RISKS-9.26](#))**

<stevev@chemstor.uoregon.edu>

Fri, 22 Sep 89 12:43:09 PDT

In RISKS-DIGEST 9.27, Will Martin asks:

>Does anyone know if this was one of the built-in magic-number  
>date breakdowns that have previously been mentioned on RISKS? ...

I'm sure that many people will respond to Will Martin's question. My lucky guess was that September 19, 1989 was 32767 days past a certain magic date, and I was off by one: September 19, 1989 is 32768 days past January 1, 1900. I'm shocked that the programmers for this system didn't think it would be used all the way into 1989, or even worse didn't consider how long it would be used at all.

The only other date limit that I know of is the UNIX time() limit of January 19, 2038 at 3:14:08 AM, when the value returned by time() will become negative if you treat it as a long. If we start treating the value returned by time() as an unsigned long, we push the magic moment back to February 7, 2106 at 6:28:16 AM.

All calculations were performed on my trusty HP-41CV with its time module, which stores alarm times as the number of seconds past midnight, January 1, 1900. Therefore, it can only represent times up to November 20, 2216, 5:46:39 PM. However, the programmers put in a software limitation of December 31, 2199 on times. This means that my HP-41CV clock will work longer than UNIX clocks without modification; not bad for a handheld computer that's showing its age even now.

Steve VanDevender

[Also noted by Amos Shapir (amos@taux01.nsc.com), who added:  
The risk of using 16-bit integers raises its ugly head again! (I wonder how many of these are still left lurking in old code...) Amos]

## **Computers, Planning, and Common Sense**

*John (J.G.) Mainwaring <CRM312A@BNR.CA>*

*Fri, 22 Sep 89 10:57:00 EDT*

I've recently seen reports of the proposed new Canadian goods and services tax which raise some disturbing questions. It appears that a major part of the proposal is to levy the tax on essentially all occasions when goods or services are sold, and hence to make tax collectors of small businesses such as piano teachers and people who do house cleaning. Of course, such people are already expected to pay income tax. The new proposal seems to be that they should also collect 9% off the top and send that to the friendly feds without waiting for April.

I somehow doubt if the visionary stupidity necessary to develop such a proposal to the point of law could have existed unaided by computers. I have no inside contacts in the Canadian finance department, but I envisage beaurocrats working over spreadsheets projecting total annual cash flows, no doubt consolidating all the char ladies in the country into one cell, and eagerly taking the results to weekly 5 minute sessions with the minister, refining all the guesses until the spreadsheet projects exactly what the minister wants to hear.

The beauty of a spreadsheet is that it doesn't require any common sense to operate. I'm sure that if it occurred to anyone to question the validity of lumping all the char ladies into one cell, he kept it to himself if he valued his career. After all, it should be easy enough for the char ladies to change the accounting packages on their PCs to deal with the new tax, and surely they would have no trouble delivering their collections by electronic funds transfer at essentially no cost to anyone - in fact, surely, time spent thinking about the char ladies at all was time wasted?

I'm not sure what one can hope to do about this sort of thing. I suppose ethics and social responsibility courses at university might help, but it may be too much to hope that government officials would concern themselves with such issues, even if we could get them into computer science curricula. Perhaps all we can hope is that our universities will find ways of increasing the small minority of all their graduates in whom they have developed the habit of occasionally thinking about what they think.

It should be obvious that these views do not represent those of my employer, or probably even myself on a sunnier day.

---

## **Synchronizing Clocks**

*<Boebert.Grapevine@DOCKMASTER.NCSC.MIL>*

*Fri, 22 Sep 89 12:35 EDT*

I cannot resist adding a note of industrial archeology to this discussion. People interested in how grandpa solved these problems should look into the design of the Synchronome clock, invented in the 1920's by one F. Hope-Jones. This consisted of a master pendulum unit (accurate to a second a year or so) electrically driving any number of slave dials. One ran as a siderial clock at

Greenwich from 1926 to 1935 without failure, a total of 284 million swings of the pendulum. Plans and instructions for making one of these magnificent beasts can be found in the old Scientific American "Amateur Telescope Making" series, Book Two, pp 427-446.

Gears and casting sets used to be available to amateurs from the (presumably) long-gone supplier. [The Synchronome Co., Alperton, Wembley, Middlesex, England is given as the 1935 address, in case any of our British Correspondents wish to go hunting for the site.] Today you would have to gain access to gear cutting machinery; the castings (mainly brackets) could be built up from bar stock using modern adhesives.

---

### ✉ **Re: Risks of Distributed Systems ([RISKS-9.26](#))**

*Sung Kwon Chung <sung@june.cs.washington.edu>*

*Thu, 21 Sep 89 20:35:00 -0700*

>..... This message is an example of asynchronous inter process  
>communication. I can guarantee you that i'm doing other things until you  
>respond or acknowledge (or this message gets dropped in a bit bucket somewhere)  
>and neither RPC nor the rendezvous allows that. ....

This is a rather common misunderstanding (at least) of RPC. With the RPC model, the idea is to separate concurrency from communication mechanism. If there are concurrent activities (e.g., sending-message-receiving-reply and doing-other-work), each of them can be encapsulated in a concurrency unit (process or thread) while communication is done synchronously by RPCs. In fact, it's the very synchronous nature which makes a lot of things simple in such a situation. So please don't tout RPC is bad because of its synchronousness.

---

### ✉ **Master clocks, etc.**

*<eddie.caplan@H.GP.CS.CMU.EDU>*

*Fri, 22 Sep 89 15:49:39 EDT*

In [RISKS 9.27](#), the Peters Jones and Neumann suggested ways of faking a distributed performance of Beethoven's 9th so that it would appear to be synchronized.

Film-music recording has a virtually identical problem. Here, it is critical that the music is precisely synchronized with the action onscreen. Rather than depending on the conductor for cues, each musician has her own headphone and listens to a click track: one electronic click for each musical "beat". The film-music conductor's job is then reduced to course-grain musical issues, such as volume balancing.

(This itself is an exaggeration of the traditional conductor/performer relationship, wherein the performer takes care of the fine-grain details of her particular instrument while the conductor concerns herself with the orchestral sound as a whole.)

For the Beethoven example, you would need <n> copies of a common click track which a local conductor would have the responsibility of following. Now the problem has been reduced to starting the performances "together". I quote "together" because to make the final performance sound synchronized, the click tracks startup would have to be staggered to overcome the satellite delays.

Finally, I think that this sort of synchronization has a lot of precedent in human endeavors. Consider trapeze artists who get synchronized at the beginning of a complicated stunt and must then rely on their own "internal clock" to be at the right place at the right time. Same for well-tuned sports teams.

---

### **✂ ISO 9001 accreditation**

*Martyn Thomas <mct@praxis.UUCP>  
Fri, 22 Sep 89 10:36:17 BST*

Jon Jacky asks for UK input on the ISO 9000 accreditation system.

ISO 9000 is the international standard for quality management systems. It does not define a system, it defines what a system must contain. ISO 9000 is actually a series of standards, and ISO 9001 covers all of design, manufacture, test and maintenance.

ISO 9001 is not specific to software - it is generic, and needs to be interpreted for each industry (or "economic sector"). It is based on British Standard BS 5750. The EC (European Commission) has directed that each sector should introduce a "sector certification scheme" to certify compliance with ISO 9000/9001. In the UK the software sector certification scheme will be called TickIT. [ just the tickit ... getting your tickit ... ...]

In the UK the BSI (British Standards Institute) has run a Registered Firms Scheme since 1979. To get BSI accreditation you have to have in place a quality management system which complies with BS5750 (now ISO 9001), and BSI audit you to ensure that throughout your organisation, every project and activity complies with your quality management standards in every respect. It's fairly tough to get.

To retain your registered firm status, you have to agree that BSI auditors can come in to the company without notice (we get 24 hours, usually) up to four times a year (we have had three each year) and repeat the spot audit. Typically they may ask what projects are active, and inspect the current list; choose a project and look at the latest status report; select a recent deliverable and look at the review reports; select an identified defect and demand evidence that the defect was corrected before delivery. Or they may pick a standard and look at how it has been applied on several current projects across the company. If they find discrepancies they insist that they are corrected, and they may withdraw accreditation.

It's good consultancy - ISO 9001 is a \*process\* standard, and the Praxis quality management system is heavily based round formal reviewing, so it

seems right that the application of the quality standards should themselves be subject to formal independent review.

Some clients take comfort from the accreditation and do not themselves audit our standards; some make BS 5750 mandatory in requests for tender. The EC will mandate ISO 9001 compliance in all public procurement at some point in the future.

And yes, before someone else points it out, it is Praxis that advertises as "the first systems house to achieve BS 5750 (ISO 9001) certification for all software development". We believe in formal QA as an essential component of software engineering, so we built a company round it.

If anyone wants more details, email me for some article reprints.

--

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK.

Tel: +44-225-444700. Email: ...!uunet!mcvax!ukc!praxis!mct

---

## ✂ Toxic Spill at the Department of Education

Joe Pujals <joep@caldwr.ucdavis.edu>

Fri, 22 Sep 89 15:20:40 pdt

The following is a description of a toxic spill that came close to having disastrous consequences for the California Department of Education. The State learned a lot from this experience and I thought others might find it interesting.

Joe Pujals, State Information Security Manager, Office of Information Technology, 915 L Street, Sixth Floor, Sacramento, CA 95814, (916) 445-1777, ...UCBVAX!UCDAVIA!CALDWR!JOEP

### THE EVENT

At 3:02 AM, Tuesday, February 21, an electrical switch located in a vault in the garage of the California Department of Education arced. The resulting explosion spewed 10 gallons of coolant oil containing polychlorinated biphenyl (PCB) through the electrical equipment vault. The loss of the switch and associated transformer was immediately noted in the control room of the Sacramento Municipal Utility District (SMUD) and a repair crew was dispatched to the trouble area.

Three minutes later, at 3:05 AM, heat and smoke sensors located in a computer room on the third floor of the building activated. The fire detection system sounded an alarm at the office of the California State Police. Following procedure in responding to the alarm, State Police called the fire department. In addition they called two Department of Education Supervisors, telling them that the fire detection system in the computer room had alarmed and requesting that they send personnel with appropriate keys to the building immediately. A passing taxi cab driver, hearing the explosion and seeing the smoke, also reported the incident to his dispatcher who in turn called the fire department.

By the time Department of Education employees arrived, approximately 40 minutes later, the smoke had cleared and locks to the garage and electrical vault had been cut. Fireman and SMUD crews had determined that there was no immediate danger from fire or loose electrical wiring.

The switch and transformer involved in the incident also provided power to the State Office Building one (Jesse Unruh Building) located one block away. The loss of power forced closure of that building until approximately 1:00 PM that afternoon. The California State Treasurer, Department of General Services and several other agencies were affected by the power outage.

The fire department had cordoned off the building to keep all but emergency personnel away. Education personnel gave fire department personnel their keys to the 3rd floor computer room and requested that they check for a fire in that area since the fire detection system had sounded. Firemen dressed in protective clothing went to the computer room. On entering, they did not see any smoke and they noted that the room temperature was normal.

The computer at the department of education consists of a TANDEM EXT25 computer, printers and terminals. The computer is used as a remote processor and print driver. Data files are maintained and computer processing is done at one of the State's two major computing centers located a few miles away. The department has approximately 475 personal computers in the building that are mainly used as productivity enhancement tools. The department spokesman indicated that some production jobs were done on microcomputers but were not sure how many applications or what they were. However, they did feel that the impact to the department, if they should be lost, would be minor.

Within hours, SMUD called the American Environment Management Co. to begin the cleanup and PCB decontamination process of the electrical vault and garage area.

Because this was an industrial accident CAL-OSHA was called. CAL-OSHA recognized that there could be additional problems associated with the PCB spill. PCB produces the carcinogens, dioxin (polychlorinated dibenzo dioxins) and furan (polychlorinated dibenzo furan), when subjected to high heat. At this time, it was unknown if the heat generated by the arcing and subsequent explosion was sufficient to generate dioxin. One other nagging question raised concerns: what had set off the fire detection system in the computer room? Was it toxic material or had the sensors been activated accidentally? At the time of the explosion, the air conditioning system in the computer room and in another computer support area had been operating. Had toxic material been sucked into the return air intake and contaminated other parts of the building?

SMUD representatives at first believed that the toxic material had been contained in the electrical vault but could not explain the coincidental activation of the fire detection system. Examination of the vault revealed that there was space between holes cut in the vault for conduit and the conduit which carried the electrical cables. It was possible for toxic material to have escaped through the gap. The conduit lead into switching equipment in an adjoining room. After passing through the switching equipment power was transferred to the electrical closets located on each of the five floors directly above the switching equipment room.

Toxic experts from the Department of Health Services were called for advice. A consensus was reached that extensive tests would have to be conducted to insure that the building was safe before employees could be allowed to return. Tests were started immediately. Test material was taken from around the holes cut into the electrical vault and from various areas throughout the building, including the computer room. The tests conducted were extensive and would not be completed before Saturday, February 25th, five days following the toxic spill.

#### MANAGEMENT'S RESPONSE

Within a few hours of the incident, it was recognized that normal operations of the Department of Education's staff housed in the affected building could not resume that day. The decision was made to inform employees to remain at home. Critical management staff were told to report to another location of the Department of Education, some blocks away, to begin the recovery planning process.

Space was cleared at the new location for the director and executive staff. Training rooms and additional space in the same building were obtained from the building owners and from a local University to house the essential displaced staff.

A public information office established a media information center in order to provide accurate and timely information to radio, television and newspaper reporters. One of the first and most important steps was to enlist the aid of the radio and television stations to make announcements requesting people to stay at home. The announcements also contained a special telephone number for emergency information. The special number was for a voice mail system.

The voice mail system proved to be one of the most valuable tools in providing staff with information. The voice mail system, capable of handling 50 incoming calls at a time, handled approximately 2500 during a seven hour period. This is considered to be a volume of calls handled in 53 hours of normal operation.

As is normal in an emergency, the situation is not always clear, information is not always timely and new problems always seem to appear from nowhere. The possible release of carcinogenic toxic substances, such as PCB or much more dangerous dioxin and furan, in a public building was considered by the various emergency response offices to be a unique event. As a result, there was not much past experience to guide the authorities in their actions. Because of the many unknowns concerning the toxic spill, the decision was reached to be cautious in the reestablishment of normal operations in the building. Extensive testing would be required, and that would take time. If the tests proved to be positive, that is, if toxic elements were found in other parts of the building, a relocation of personnel to a new site would be necessary.

The Space Management Office of the Department of General Services was alerted to the problem and was asked to begin the process of finding space for approximately 650 people. Potentially usable space was found, but lease negotiations were held off until the results of the tests were determined.

The immediate problem was what to do with 590 people until normal operations

could be reestablished. Of the 590 staff, 150 people were on business trips throughout the State and would not represent a placement problem until they returned. The department examined travel plans and attempted to reschedule planned business where it was reasonable. Others were asked to take scheduled vacations. Where it was practical, staff were directed to do their normal office work at alternate sites within the department or other agencies. The remaining employees were simply put on administrative leave. Since the decisions affected both professional staff as well as nonprofessional staff, the department included the California State Employees Association when bargaining unit staff were involved.

By the end of the second day, the department was reasonably sure that toxic substances had been contained but could not be certain until more definitive tests were concluded. If the toxic material had not been contained as it appeared, but had indeed spread to the rest of the building then there would be a number of new questions to be answered. For example, could the tons of documents, paper files, magnetic tapes and floppy diskettes be decontaminated or would they simply be buried? Could the hundreds of microcomputers, terminals, typewriters and other pieces of office equipment be decontaminated or would they have to be replaced. How do you, or should you, replace information contained in the paper files? These and many more questions would have to be answered in the next few days if any test came back positive.

On Saturday afternoon the results of the tests came in; they were negative. Employees could reenter the building on Monday.

The cost of this disaster probably will not be known for a few weeks. It will take time to calculate the cost of lost time.

It is interesting to note that in the course of the week the process of cleanup and recovery had involved the Sacramento Municipal Utility District, the American Environment Management Co., the Sacramento Fire Department, the Toxic Substances Control Division and Hazardous Materials Laboratories of the Department of Health Services, CAL-OSHA, Sacramento County, the State Architect, the divisions of Buildings and Grounds, and Space Management from the Department of General Services, and the California State Employees Association. If toxic tests had been positive, there would have been many more organizations involved and many more very difficult decisions to be made before recovery could have been completed.

#### CLOSING COMMENTS

PCB, dioxin, and furan were found in the switch equipment room and in the electrical closets on the floor above. But no trace of the toxic material was found outside of the electrical closets. Since the conduit passed through all six floors, SMUD has been asked to decontaminate the electrical closets on each floor.

The reason that the fire detection system activated will probably never be known. It is assumed that the system was activated as a result of fluctuations in the electrical power.



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 9: Issue 29

Monday 25 September 1989

## Contents

- [Computerized fingerprint system has human failure](#)  
[Dave Suess](#)
- [Computerized translation strikes again](#)  
[Joe Morris](#)
- [Loose wires](#)  
[Desmond Andigo via John Leonard](#)
- [Software \\*IS\\* an abstraction](#)  
[Bob Estell](#)
- [Yes, the power grid IS getting less reliable](#)  
[Bruce Hamilton](#)
- [Computers, Planning, and Common Sense](#)  
[Richard O'Keefe](#)
- [Simulated aircraft emergencies](#)  
[John Mackin](#)
- [Re: Software Accreditation](#)  
[Richard Threadgill](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✉ **Computerized fingerprint system has human failure**

*Dave Suess (CSL) <zeus@aerospace.aero.org>*  
*Mon, 25 Sep 89 07:37:34 -0700*

(From the Easy Reader, a weekly newspaper in the South Bay section of L.A.)

A Redondo Beach resident, Martin Lee Dement, spent almost two years in a Los Angeles County jail because of a botched use of the state's computerized fingerprint-matching system, ALPS (Automated Latent Print System). Arrested for robbing a Radio Shack, Dement was jailed, his girlfriend sold her condo to raise money for defense lawyers, and the experience may have contributed to his recidivism (he had been an habitual offender, and speculation is that the 21 months he spent incarcerated wiped out the progress he had been making since his last release).

There was much thrashing by two consecutive public defenders and finally attorney Charles Maple (who defended Onion Field killer Gregory Powell) to get the D.A. or police departments involved to match prints lifted at the scene of the robbery with those of another suspect, Dennis Passon, also arrested about the same time, for a string of similar robberies (including a Radio Shack store). None of the law enforcement officials would make a direct comparison between the lifted prints and those of Passon, even though they had him in custody. Instead, the lifted prints were sent through ALPS --- and no match was produced.

Finally, two weeks into Dement's trial, the prints were produced and the judge ordered a comparison to be made with those of Passon. A match was immediately obvious, and charges against Dement were dropped, after he had spent 21 months in jail. The D.A., Julie Sulman, blamed ALPS, which had just come online. Investigators had just assumed that since Passon had an extensive criminal record that his prints would be online, also. Sulman said, "I think we made an erroneous assumption that Passon wasn't the guy because he would have been in ALPS ... and we were wrong."

Attorney Maple said recently that "ALPS is bull\*\*\*\* and it doesn't take care of anything."

[Censorship \*\*\*\* is mine. This is a family newsgroup. PGN]

---

## **Computerized translation strikes again**

*jcmorris@mitre.arpa <Joe Morris>  
Sat, 23 Sep 89 18:59:24 EDT*

[From page R6 of the Wall\_Street\_Journal\_, Friday, 22 September 1989 comes yet another story of the perils of computerized translation of natural languages. The text below appeared in a sidebar to a story about the problems encountered in trying to resolve differences between European countries preparing for the 1992 amalgamation into the EC...]

### TOWERING BABBLE

Automatic translation system proves that to err isn't just human

Interpretation and translation gobble up a huge hunk of EC's central budget, so the Eurocrats have been trying to save money by using an automatic translation system. Systran is its name. Bloopers are its game.

To the unconcealed delight of those whose jobs it first appeared to threaten, Systran, acquired from the U.S. Navy about 10 years ago, still has a bit to learn about French-English translation. A few howlers:

\* Commission President Jacques Delors asked in French whether he could address a certain committee. Systran had him asking whether he could "expose himself to the committee."

\* Crown Prince Jean of Luxembourg, invited to offer a royal page of prose to the computer, used the words \_nous\_avions\_, which in context only

meant "we had." Systran made it "us airplanes."

\* In one screed about farming, the writer used the phrase *\_les agriculteurs\_ \_vis\_a\_vis\_de\_la\_politique\_agricole\_commune\_*, which means "farmers, in the light of common agricultural policy..." Systran, suffering either a blown microprocessor or an uncanny flash of insight, rendered it as "farmers live to screw the common agricultural policy."

[The article goes on for another nine column inches discussing non-computer related problems of translation, which are significant. In the headquarters of the Council of Ministers there are about 2000 bureaucrats, half of whom are translators.]

---

### **✂ loose wires**

*John Leonard <john@robots.oxford.ac.uk>*

*Mon, 25 Sep 89 19:58:26 BST*

A friend of mine regularly reads RISKS which I print out for him (He is not on a network.) He has asked me to pass on the following message which he typed in on his pc and downloaded onto our system.

DISCLAIMER: I would like to point out that no members of this group have any connection with the author or his story, except as a friend.

-----

Having read with interest the articles in [RISKS 9.26](#) and 9.27 about loose wires, I thought I would readers might like to share my own story of a similar incidence.

Some years ago, I was exploring in Africa hoping to trace a long-lost relative; when due to a peculiar set of events I found myself in a great deal of trouble. I was part of a team of explorers: all of us searching for our own and the other team-members relatives.

We each had a portable radio and could be contacted by another team-member who was stationed at "base camp". Anyone who discovered anything interesting was supposed to radio the base camp, the news being relayed to the rest of the team when they contacted base camp.

The radio I had was supposed to be what was then a very modern design incorporating a primitive computer which was supposed to switch in the full power when a signal was received, conserving energy while no information transfer was occurring. Unfortunately, after a couple of weeks, when the novelty of using the radio to call up for regular status reports had worn off, one of the wires on the radio worked itself loose and as a result, while I was capable of radioing base camp, they could not contact me as the power was not sufficient to raise me without the computer working properly.

I did not call base camp for several days/weeks (I forget how long it was). Imagine my surprise when I did get to call, however, and discovered the

following:

While I had continued my search, the other members of the team had returned to camp, some successful, but in the main unsuccessful. I was the only one left searching and the team leader decided to call me back. Unfortunately, my radio did not respond and so, fearing the worst, the remainder of the team set out to find me. By the time I next called the camp, the whole team was searching for me, searching the many miles of land in which I could possibly be.

During their search, one of the team members (a chap called Maurice [I don't remember the surname]) was bitten in his sleep by a sloth (he alone in the team thought he was safer sleeping in a tree) and had to spend several weeks in hospital on our return.

Although we laughed about the whole affair afterwards, it did make us realize how dependent on the technology we were. Since then I have been understandably wary of computers (though I do now own a small wordprocessor) ... and have taken a keen interest in discussion groups which talk about the potential problems of computers.

Desmond Andigo (Retired Businessman)

---

### **✂ Software \*IS\* an abstraction**

*"FIDLER::ESTELL" <estell%fidler.decnet@nwc.navy.mil>  
25 Sep 89 13:09:00 PDT*

How can we study "real software" for verification, among other purposes? Can we read a listing in some programming language? Can we read a memory dump - if that is not a lost art? Can we monitor execution under control of an interpreting debugger?

I submit that these and other forms of "studying software" amount to the study of an abstraction of what really counts; viz. the system. The software, without a processor to run it, is but an abstraction of what the programmer wants the system to do; the hardware, without the software to guide it, is but a potentially versatile idle tool.

The system runs in real time; i.e., as fast as the processor and its input/output allow. When one slows that process down to the pace that a human can observe in detail, subtle timing problems behave differently.

That is not to say that interesting subsets of a system cannot be isolated into time invariant forms, and then analyzed rather thoroughly. And that is very valuable; it has given us better compilers and math libraries, among other things. But systems that deal with things that directly affect human life, like hospital monitors, and flight controllers, run in real time. Yes, it is far better to build them insofar as possible with parts that are verified; but the whole remains an abstraction, until we develop other tools which may depend on our first developing other paradigms.

---

**✂ Yes, the power grid IS getting less reliable**

*Bruce Hamilton <Hamilton.osbuSouth@Xerox.COM>*

*24 Sep 89 22:23:46 PDT (Sunday)*

Since the reliability of the power system relates directly to the reliability of many computer systems, the following info is probably of interest.

I spoke with a friend who used to be in charge of building large power projects for Southern California Edison (SCE). He said that, due to increasing competition and decreasing ROI, over the past ten years or so SCE has planned its power grid to "N-1" standards, whereas previously they planned to "N-2". "N-1" means they can lose only one major transmission line without a major system blackout. He added that even "N-1" is marginal in some cases.

Of course, they DID learn a lot from the big (1964?) blackout in the Northeast, where the system wasn't smart enough to partition itself in the face of unexpected overloads, and so the whole system went black and huge generator bearings melted down and were out of commission for months because the power plants had no UPS's to pump lubricating oil.

Still, my experience is that most blackouts are small, localized ones due to things like a car knocking down a transformer. We seem to suffer three or four per year here in El Segundo, CA.

In summary: keep buying those UPS's for your data center.

--Bruce 213/333-8075

---

**✂ Subject: Computers, Planning, and Common Sense (Re: [RISKS-9.28](#))**

*Richard O'Keefe <ok@cs.mu.oz.au>*

*25 Sep 89 05:20:58 GMT*

A Goods and Services Tax has been in operation in New Zealand for several years now. The scale was recently lifted from 10% to 12.5%. Somehow this is supposed to be compatible with the Labour(!?) commitment to free markets and reduced government intervention.

As near as I can figure out, if Farmer A trades a pig to Farmer B for Farmer B's cabbages, they both owe the government 10% (now 12.5%) of the monetary value of the deal.

The bottom-line tax-payer just loses money, although personal income tax levels were reduced, so it more or less evened out. Everyone above that layer pays in paperwork. The theory is that each item should have GST paid on it once, so that GST on inputs can be claimed back from GST on outputs.

> I somehow doubt if the visionary stupidity necessary to develop such a  
> proposal to the point of law could have existed unaided by computers.

I don't know what's involved inside the Government, but charladies don't

need spreadsheets to carry out their paperwork.

My objection to GST is that it hits the poor relatively harder than the rich, but this is apparently compatible with NZ Labour's ideals.

---

## ✈ Simulated aircraft emergencies

John Mackin <john@cs.su.oz.AU>

Sun, 24 Sep 89 22:26:44 +1000

In [RISKS-9.25](#), Alan Rosenthal says:

- > The trade-offs during practice and emergencies are different, and should be.
- > It's sad that this means that you can't really simulate emergencies fully.
- > Nevertheless, it's *\*true\** that this means that you can't really simulate
- > emergencies fully.

This is quite true. The whole point that makes this idea unworkable is that you are putting a multi-million dollar aircraft (and the lives of its passengers, if passengers are being carried -- and I assume they would be, as the original proposal mentioned "routine flight") at risk, simply for training purposes. This is not acceptable.

On the other hand, when they are available, simulated emergencies can be a very effective tool for pilot training. I will certainly never forget the first time I was subjected to one: climbing out from the airport on perhaps my sixth or seventh flight as a beginning pilot, I reached the altitude at which I had been taught to conduct after-takeoff checks. These were quite simple: speaking aloud, they went: "Flaps up (pointing at flap indicator), fuel pump off (turning it off), fuel pressure holding (pointing at fuel pressure gauge), engine instruments green (pointing at each in turn)." About ten seconds later, my instructor said: "Did you forget something?" I knew I hadn't, but I also knew the right thing to do: start the checks again from the beginning. "Flaps up, fuel pump off (reaching down and pushing the switch off, where it already was), fuel pressure..." The fuel pressure gauge was reading zero. "NO FUEL PRESSURE", I shouted, practically breaking my hand turning the auxiliary (electric) fuel pump back on. I was all ready to push the nose down when the engine failed, and for a fraction of a second I took my eyes off the fuel pressure gauge, which wasn't coming up, to look at my instructor. He was gazing outside, cool as a cucumber. I couldn't understand it. After another fifteen seconds or so I began to catch on. The gauge still read zero, but there was no way the engine was still running with no fuel pressure. "OK, Eric, what did you do?" He pointed to the circuit-breaker panel, where one of them was sticking out. I checked that it was the right one and reset it. Then he said to me: "When you check an instrument, don't just glance at it. Take a good look, five seconds at least. It's not just the instantaneous reading you want to see: there may be a visible rate of change, and if so, you want to know about it."

It certainly drove the point home, and I always follow that practice. But you can't do that to the pilot of a B747 en route.

John.

---

## ✈ Re: Software Accreditation

Richard Threadgill <[richardt@mica.berkeley.edu](mailto:richardt@mica.berkeley.edu)>  
Fri, 15 Sep 89 20:25:14 PDT

I would point to the vast abuses in the medical, legal, and teaching professions as reasons why some form of accreditation *should not* be created. The legal process has been codified to such a degree that the only way to challenge the legal profession is to convince a lawyer to blacklist another lawyer; the medical and teaching professions have both had vendettas with professionals who were not politically correct, while allowing *many* abuses to go unchecked.

We come down to a very simple problem if we wish to teach ethics at all:

Whose ethics do we teach?

Meanwhile, of course, we are ignoring one very simple fact: Data Theft and industrial espionage and security are all highly lucrative fields... and they are becoming more so. With many of the wealthiest companies in this country resorting to highly illegal tactics on a regular basis, can we realistically think that we will stem the tide by saying "nice programmers don't do that?" Especially when these are *still* some of our most talented people!

RichardT



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

**Volume 9: Issue 30**

**Monday 2 October 1989**

## Contents

- [The Cuckoo's Egg](#)  
[Cliff Stoll](#)
- [Internet cracker on the loose](#)  
[Barry Lustig](#)
- [Late night system administration == trouble on SunOS 4.x](#)  
[Angela Marie Thomas](#)
- [Date manipulation and end of millennia](#)  
[Pete Lucas](#)
- [Re: An interesting answer to the distributed time problem](#)  
[Randall Davis](#)
- [Re: Man-Machine Failure at 1989 World Rowing Championships](#)  
[Randall Davis](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **The Cuckoo's Egg**

*Cliff Stoll <[cliff%cf253@harvard.harvard.edu](mailto:cliff%cf253@harvard.harvard.edu)>*  
*Sat, 30 Sep 89 23:59:05 edt*

The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage,  
by Cliff Stoll, Doubleday, 1989, ISBN 0-385-24946-2      \$19.95

Book Review by Louise Bernikow, *Cosmopolitan*, Oct. 1989

Here's a first -- the true story of a man who notices a seventy-five cent discrepancy in a computer's accounting system and runs the error down until it leads to a real live spy ring. Even if you don't know a byte from a bagel, this book will grip you on page one and hold you as ferociously as the best mystery stories.

It is astrophysicist-turned-systems-manager Cliff Stoll's first week on the job at a lab in Berkeley, California. The error turns up, and he tries to figure out why, partly as an exercise in learning about the computer system he's going to be working with. Almost immediately, he discovers that somebody had been

breaking into the computer network using a fake password. That discovery leads him to other break-ins in other computers, including some in military installations. He alerts the FBI, which, since he has lost neither half a million dollars nor any classified information, says, "Go away, kid."

Stoll presses on, sleeping under his desk at night, monitoring the system -- a hound waiting for the fox to come out in the open. There is suspense aplenty, but it's the intensely human, often funny voice of the man on the trail that makes this book so wonderful. Stoll's girlfriend, Martha, a law student, seems like one smart and delightful cookie, and she puts up with his obsession pretty well. In the end, Stoll becomes a national hero. The play-by-play is nothing short of fascinating.

---

### **✂ Internet cracker on the loose**

<barry@ads.com>

Mon, 02 Oct 89 14:52:08 PST

There is a cracker on the loose in the internet. This is the information I have so far. Traces of the cracker were found at the Institute for Advanced Studies in Princeton. He also left traces at one of the Super computer centers. Both CERT and the FBI have been called.

The technique that is being used is as follows:

- 1) He has a modified telnet that tries a list passwords on accounts. Username forwards and backwards, username + pw, etc.
- 2) He seems to have a program call "ret", that is breaking into root.
- 3) He seems to be getting a list of victim machines via people's .rhosts files.
- 4) He copies password files to the machines that he is currently working from.
- 5) He is good about cleaning up after himself. He zeros out log files and other traces of himself.
- 6) The breakins are occurring bwtween 10pm Sunday night and 8am Monday morning.
- 7) He seems to bring along a text file of security holes to the machines he breaks into.
- 8) Backtracing the network connections seem to point to the Boston area as a base of operations.

The sys admin at IAS found a directory with the name ".. " (dot dot space space). The files I mentioned above were found in this directory.

Barry Lustig, Advanced Decision Systems barry@ads.com (415) 960-7300

---

### **☛ Late night system administration == trouble on SunOS 4.x**

Angela Marie Thomas <thomas@shire.cs.psu.edu>

Sat, 30 Sep 89 01:33:31 EDT

It's another late night of system administration. Tonight the task is time consuming, but relatively simple: Repartition the disks on a Sun4/280 running 4.0.3 to distribute the load to a new disk. No big deal.

I partitioned the new disk and dump|restore'd most of the stuff from the old disk onto it and rebooted off of the new disk. I then proceeded to repartition and newfs the old disk. No problems so far.

I was about to dump|restore /usr from the new disk back to the old disk (yes, / and /usr are on two different disks) so I mounted xy0g onto /mnt. At least, that's what I \*intended\* to do. My fingers typed "mount /dev/xy0a /usr" instead. OOPS! Well, no real harm done. I'll just pop over to /sbin and umount the device. WRONG! It seems that /sbin has enough programs in it to get you into trouble, but not enough to get you out of it. No dump, no restore, no umount. I couldn't even sync;sync;halt the system. Oh, mount is there. I could mount more newly newfs'd filesystems onto /usr until my face turned blue. I can't believe it. It was as if I had just stumbled into a cul-de-sac. The only damage done was to me, not the machine. Sigh.

Sun, if you're listening, please, please, please put statically linked umount, dump, restore, sync and halt in /sbin. Nine times out of ten, those are the programs I want when I \*need\* /sbin.

Angela Thomas                      NSFNET: thomas@shire.cs.psu.edu

---

### **☛ Date manipulation and end of millennia**

"Pete Lucas, NERC-TLC Swindon U.K." <PJML@ibma.nerc-wallingford.ac.uk>

Thu, 28 Sep 89 15:51:09 BST

Date processing; anyone interested in digging out some definitive works should try the following:

Ohms B.G (1986) 'Computer processing of dates outside the twentieth century'  
2

IBM systems journal vol 25 no.

Uspensky J.V. and Heaslet M.A. (1939) 'Elementary Number Theory'. Mcgraw-Hill

Whitrow G.J. (1988) 'Time in History' Oxford University Press, Oxford U.K.

Much of the relevant work in Whitrow (1988) is based on the works of the French astronomer Jean-Baptiste Delambre (1749-1822).

Anybody who is interested, I have robust examples of routines for the manipulation of dates, and examples of routines (written in REXX but easily translated to FORTRAN if you so desire).

It has been suggested that if the year is divisible by 4000 then it should NOT be considered a leap-year. Anyone writing code that's likely to be around 2000 years hence???

>-=Pete=-<

---

**✂ Re: An interesting answer to the distributed time problem ([RISKS-9.26](#))**

*Randall Davis <davis@ai.mit.edu>*

*Thu, 21 Sep 89 20:27:33 edt*

> Take any of the thousands of closed circuit TVs in the

\*\*\*\*\*

> hospital and set it to channel 6 and you get a picture of a clock.

> Somewhere there is a TV camera pointed at a good old sweep-secondhand

> analog clock, and that's what you see on

> channel 6. Sometimes low-tech solutions are the best.

Thousands of TVs? An expensive television camera doing nothing but sitting there focused on a clock? All those cables, monitors, all that power, bandwidth to burn on the network, etc.?

And you call this a **\*\*low tech\*\*** solution because the clock is analog? Egad. Perspectives have been rather skewed.

(Low tech would be a human being walking around with a chronometer re-setting all those clocks by hand.)

---

**✂ Re: Man-Machine Failure at 1989 World Rowing Championships ([RISKS-9.26](#))**

*Randall Davis <davis@ai.mit.edu>*

*Thu Sep 21 21:29:32 1989*

On the other hand, I am surprised that in a sport so close to being natural (apart from computer designed shells) a computer would be permitted on-board.

A "natural" sport? With exotic materials used in the fixtures and in some oars, tanks designed as artificial rivers to row in during the winter, nautilus machines for strength training, attention to nutrition, etc., etc.... Sports haven't been "natural" since the Greeks ran the Olympics in the buff.

Technology knows no bounds! PGN]

Indeed, much like imagination.

[I think no sports are natural anymore. The use of computers in baseball is startling. Basketball may be fairly natural. However, with all the steroids, drugs, etc., however, one is never sure what is going on. 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 9: Issue 31**

**Wednesday 4 October 1989**

## Contents

- [Computer multiplies taxable earnings by 100](#)  
[Rodney Hoffman](#)
- [Hackwatch spokesman charged](#)  
[Dave Horsfall](#)
- [Re: Internet cracker on the loose](#)  
[Randy Buckland](#)
- [Re: Hospital problems due to software bug](#)  
[Mike Kimura](#)
- [Re: Date manipulation and end of millennia](#)  
[Henry Spencer](#)
- [Re: Clock-watching](#)  
[George L. Sicherman](#)
- [9-digit precision](#)  
[Gideon Yuval](#)
- [The Risks of Crossing the Tracks \(Railroad Crossing Gate Technology\)](#)  
[Jean- David Beyer](#)  
[Laurence Larry Sheldon](#)  
[Richard L. Piazza via Chuck Weinstock](#)
- [Fifth Annual Computer Security Applications Conference](#)  
[Marshall D. Abrams](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ***⚡* Computer multiplies taxable earnings by 100**

*Rodney Hoffman* <[Hoffman.ElSegundo@Xerox.com](mailto:Hoffman.ElSegundo@Xerox.com)>

4 Oct 89 07:17:53 PDT (Wednesday)

>From the 'Los Angeles Times' 2-Oct-89:

Hundreds of independent employees who worked for Wells Fargo Co. two years ago were stunned to learn of a computer error that multiplied their earnings by 100 before passing on the information to the Internal Revenue Service. The IRS, eager to collect Uncle Sam's share, has written to the taxpayers, demanding an explanation for the discrepancies between the Wells Fargo reports and the

recipients' 1987 tax returns. "I was panicked. They moved the decimal point two places to the right," real estate appraiser Harold M. Samuelson told the Salinas Californian.

---

### **✂ Hackwatch spokesman charged**

*Dave Horsfall <dave@stcns3.stc.oz.au>*

*Wed, 4 Oct 89 09:22:35 est*

This item, taken from "Computing Australia" 2nd October, should warm the cockles of a few hearts...

``Hackwatch spokesman charged

Self-styled computer security expert Paul Dummett, alias Stuart Gill, has been charged with making false reports to the Victoria Police following an investigation into claims he made in the daily media late in 1988 and early this year. The articles often quoted Gill, introducing himself as a spokesman for either "Hackwatch" or the "DPG monitoring service".

Gill claimed hackers in Australia had gained access codes from others in the US and lifted \$US500,000 from the International Citibank, US. Other claims: credit card numbers had been posted on bulletin boards for BBS users' access; drugs, including steroids, were being sold using bulletin boards; evidence of this had been given to the police by informers; and in response, the police had raided several hackers' homes. The police, including the Criminal Investigation Bureau and the Fraud Squad's Computer Section, repeatedly denied the claims.

Gill had disappeared, but returned again on September 22 and was charged in the Frankston Magistrates' Court under his real name, Paul Dummett. According to court documents, police investigating Dummett's claims allegedly found Citibank's computer network had not been illegally accessed on its New York number as Dummett had claimed. When Dummett appeared in court his legal aid counsel Serge Sztrajt applied successfully to adjourn the case to October 20. Dummett did not enter a plea."

Dave Horsfall (VK2KFU), Alcatel STC Australia, dave@stcns3.stc.oz.AU  
dave%stcns3.stc.oz.AU@uunet.UU.NET, ...munari!stcns3.stc.oz.AU!dave

---

### **✂ Re: Internet cracker on the loose**

*Randy Buckland <rcb@ccpv1.ncsu.edu>*

*Tue, 3 Oct 89 10:00:46 EDT*

We have also been hit by this person. We managed to trace some of his activities. He broke into an account that saved it's history file and we saw some of what he did to get root access. \*\*\*\* THERE IS A SECURITY HOLE IN V3.0 ULTRIX \*\*\*\* This hole is fixed in 3.1. This problem has not

been mentioned in any DEC communications we have received. If you are running 3.0 and this person can break into a normal account, he can get root access with no trouble.

Randy Buckland rcb@ncsu.edu

---

**✂ Re: Hospital problems due to software bug ([RISKS-9.26](#))**

*Mike Kimura <MNK@draco.hac.com>*

*Mon, 2 Oct 89 18:53:59 PDT*

In RISKS-DIGEST 9.27, Will Martin wrote:

> I was hoping that someone out there has kept track of and will post a note  
> listing those magic dates for various OS's and systems. It will be a useful  
> reference for all of us.

The base time for VAX/VMS is November 17, 1858 (which is the base of the Modified Julian Day system). VAX/VMS uses 63-bit absolute time representation (negative values are delta time representations) with a 100 nanosecond granularity therefore the last absolute time value that can be represented is:

July 31, 31086 at 02:48:05.47 AM.

However, all date/time routines within VAX/VMS allow for only 4 digits for the year field so after 31-DEC-9999 the year field will look like 1-JAN-\*\*\*\*.

Mike

Michael Kimura, Hughes Aircraft Company (RSG), P.O. Box 92426 MS: R2/9A37  
Los Angeles, CA 90009 (213) 615-9775

---

**✂ Re: Date manipulation and end of millennia**

*<henry%utzoo@neat.cs.toronto.edu>*

*Tue, 3 Oct 89 11:54:18 EDT*

>It has been suggested that if the year is divisible by 4000 then it  
>should NOT be considered a leap-year. Anyone writing code that's likely  
>to be around 2000 years hence???

This is actually just a specific manifestation of the fact that calendar reform requires altering timekeeping programs to match. Leap millennia are *\*not\** officially part of the calendar, last I heard; anyone who writes code on that basis has goofed.

I do recall some amusing ads for digital watches (back when they were new) whose timekeeping was guaranteed accurate to the year 2099. That is, the designers didn't feel like allowing for leap centuries, and lucked out on the year 2000 following the same rules as normal leap years.

Henry Spencer at U of Toronto Zoology

---

**✂ Re: Clock-watching ([RISKS-9.30](#))**

George L Sicherman <gls@odyssey.att.com>

Tue, 3 Oct 89 22:17:22 EDT

In [Risks Digest 9.30](#) Randall Davis decries the practice of transmitting an image of a clock:

> Thousands of TVs? An expensive television camera doing nothing but  
> sitting there focused on a clock? All those cables, monitors, all that  
> power, bandwidth to burn on the network, etc.?

What a waste of resources indeed! That expensive equipment was meant for Geraldo Rivera, "Roseanne," and reruns of "Family Ties"--not for frivolous ends.

I can't wait till we have high-definition television....

(N.B. I do not speak for AT&T!)

Col. G. L. Sicherman

---

**✂ 9-digit precision**

Gideon Yuval <gideony@microsoft.UUCP>

Wed Oct 4 08:51:49 1989

A recent report "Macintosh S/W markets: productivity S/W review & forecast, 1998-1993" (International Data Corp, 8/89) predicts that, in 1993, the U.S will buy so many millions, nine hundred twenty-nine thousand, five hundred AND FIFTEEN dollars' worth of Mac word-processing software. The leading digits have been suppressed to protect the publisher's interests; but given that all nine digits have been published, I wouldn't trust them that far anyway. This is a reasonably expensive report (a few hundred \$) which probably affects a good many high-level management decisions.

I think this tomfoolery is relevant to comp.risks on two grounds: (1) it's a textbook demo of common sense abdicating in the face of "the computer says so"; (2) I was told "that's Excel's default-mode for output" (and -- I think -- other spreadsheets' too).

I was also told "that's what they learn in business school!". I hope not.

Gideon Yuval, gideony@microsoft.UUCP, 206-882-8080 (fax:206-883-8101;TWX:160520)

---

**✂ The Risks of Crossing the Tracks (Railroad Crossing Gate Technology)**

*Chuck Weinstock <weinstoc@SEI.CMU.EDU>  
Wed, 04 Oct 89 10:48:52 EDT*

On the day that New Jersey Transit inaugurated service to Atlantic City, there was a grade crossing accident that provoked a discussion of crossing gate technology on the newsgroup rec.railroad. It is interesting to note how an "old" industry operating in difficult conditions (equipment outside, subject to all sorts of environmental problems, not to mention vandalism) solves a safety problem.

Chuck Weinstock

>From: beyer@holin.ATT.COM (Jean-David Beyer)

I have some notes from General Railway Signal Company on railroad signalling. There are separate sections on Wayside Signals, Crossing Gate Signalling, Cab Signals, Frequency Shift Overlay Signalling, and so on.

The stuff is fool-proof, but not damn-fool proof. It cannot keep people from going around crossing gates.

If the power source of signalling goes out, signals fail to stop. If rails break, signals fail to stop. If vandals short out the rails, signals go to stop. If insulating joints fail to insulate, signals go to stop. If relays springs break, signals go to stop. If relay coils open, signals go to stop. If a lamp burns out, this is detected and the least restrictive aspect more restrictive than desired is displayed. Get the idea?

However, a suitably well-informed vandal could break the rail, having previously put heavy electrical bonds around the gap, and wreck a train.

Or he could make his own code transmitters and couple them into the rails (after disabling the real ones). But it is a lot of trouble to do this without attracting the notice of the dispatcher.

Basically, when things go wrong, they fail safe. Even when someone around here bumped an extruded aluminum crossing gate so that when it went up it hit the 12500 volt 1500 ampere catenary. It melted the gate and fried a couple of relays in the control bungalow. The gates stayed down until that was fixed. On the other hand, if the gates stay down longer than an unreasonable driver thinks is a reasonable time, he will go around the gate and get hit by a train. Sometimes a train is coming the other way from one that is stopped in a station, such as at Bridge and Monmouth streets in Red Bank. An eastbound train was stopped in the station with the intersection apparently clear. The driver could not wait a few seconds (less than 60) for the train to pull out and started around the gate. Only then did he see the westbound train and stop clear of the other track. That is the kind of damn-fool proof the system is not.

Engineers must assume a signal improperly displayed is displaying the most restrictive aspect that the signal is capable of (under most conditions). Car drivers should assume that if a gate is down, that they do not have time to get around the gates. Sometimes they do, but it is a dumb thing to bet your life on.

> From: lsheldon@cup.portal.com (Laurence Larry Sheldon)

On the SP Penninsula Line (and others--it seems like) there is a white light that shines down the right-of-way in each direction--if it is a bells and lights only crossing, the light blinks in concert with one of the red lights (in many cases it is a lens in the side of the red lights case).

If there is a gate, the white light does not flash unless the gate is down.

There seems to be a rule that the train must stop (or maybe it's run dead-slow) if the white light is not blinking.

This is based on observation, not knowledge of the facts.

> From: lsheldon@cup.portal.com (Laurence Larry Sheldon)

On the SP again--if a train stops at a station (or in areas where switching activity is high) the gates open up again if the train does not cross within some time limit. The engineer has to "whistle" the gate back down (there are post-mounted microphones--actually loudspeakers-used-as- microphones) before proceeding. On some non-main line tracks there is a "STOP" sign at the pavement (White on rectangular red)--when the train gets to the stop sign, the gates come down.

> From: beyer@cbnewsh.ATT.COM (jean-david.beyer)

G.R.S. have some motion detector circuits available. I do not know if they use doppler detectors, or rate of change of signal amplitude, or what. But they are used where there is a lot of switching activity near a grade crossing. If a train starts toward a crossing at over 2 mph, the gates come down. If the train stops, the gates go back up. If the train resumes, the gates come down again. If the train reverses (goes away from the intersection), the gates stay up. Costly enough that they are not used much around here. But there is little switching on the NJ Coast Line.

I have been told that some such units estimate the speed of the train, and wait a while before putting the gates down if the train is coming slowly. This seems theoretically possible, but I have seen no written information about that.

> From: beyer@holin.ATT.COM (Jean-David Beyer)

None of the Operating Rules I have read (but I have only about a 1974 Central Railroad of New Jersey and a NORAC from early 1988) specifically discuss such lights. <<The blinking white light referred to previously...CBW<>

However, my G.R.S. notes say that if the white light does not flash (the one you can see out the side of the red flashers for motorists), the signal maintainer should be notified. (I.e., the signals are not working.)

There are rules dealing with flagging over grade crossings. I do not remember them exactly, but they deal with situations where the flagman has defeated the crossing protection (by putting a key in a lock switch) for local switching. Then he must provide flag protection until the train physically blocks the intersection (unless he can resume the crossing protection for some period of time before the train movement is resumed).

> From: rich@linus.UUCP (Richard L. Piazza)

I have noticed that the amount of time between the lowering of the gates and the actual passage of the train is sometimes VERY long. I never would go thru the gates, but I am sometimes tempted -- especially when everybody else is doing it.

I bet less people would try to go thru the gates if there was less of a time lag.

Has anybody else noticed this? Is there a standard for the amount of time that the gate must be down before the train arrives?

> From: beyer@holin.ATT.COM (Jean-David Beyer)

I think you are right: if gates went down only a short time before the arrival of the train (or, more exactly, before the train occupied the crossing), and then went up as soon as the train departed, less people would go around.

I do not know what the standard times are, but I am sure they exist. I do know that around here, they flash the lights and ring the bell for 6 seconds before the gates come down. Unless the lights and gates are coupled to the municipal traffic signals. Then they get a little more time, so the traffic signals get a chance to go red across the tracks. For ordinary crossing circuits, the gates come down when the train hits the approach track. Since, around here, no insulated joints are required for the gates (Frequency Shift Overlay circuits), the approach can be any length decided upon by the railroad. But it must be long enough so that the fastest train will get the gates down in time. Since rules prohibit speeds in excess of 79 miles per hour where there are grade crossings, you can calculate the amount of approach track needed if you know how much advance warning you need (someone who got on the tracks as the gate closed behind him needs time to get off before getting hit by the train).

But if a train is going significantly slower, the gates can be down quite a while. My "calibrated eyeball" says the approaches to the Red Bank New Jersey crossings are about 1/2 mile long.

What seems to annoy people around here is when the train is stopped in the station. The gate is down because the train is about to leave. But it may be there a while if people take a long time to get off and on. This makes people want to go around the gates. By Murphy's law, there will be an unseen train coming the other way that will hit them. Luckily, I have never seen an accident like that, but I saw a close one recently.

Also, if it has not rained for a long time, lots of potentially conductive crap builds up on the ballast. When the rain first starts, this can bring down the gates until it washes off.

When you figure that the resistance between the rails can go as low as 1/4 ohm from rain and dirt, and that the shunting resistance of the trains can go up as high as 0.06 ohm, it does not leave the signal system with a lot to work with.

Movement detectors could put the gates up if a train stops or slows down

appreciably. But they cost much more. At Long Branch, the gates are up even when the train is on the approach to the crossing, since the trains stay there to wait for the shuttle from Bay Head. To make the signal go from Restricting to Approach-Limited, the conductor operates a key in a lock that puts the gates down. This is a nuisance, but it must have been considered to be cheaper than motion detectors.

There may well be a grandfather clause that permits old stuff to be used. The railroads do not seem to have a lot of money to pay for capital improvements whenever something new comes out.

---

## **✶ Fifth Annual Computer Security Applications Conference**

*Marshall D. Abrams <abrams%vlad@gateway.mitre.org>*

*Fri, 29 Sep 89 10:50:48 -0400*

Fifth Annual Computer Security Applications Conference  
(formerly the Aerospace Computer Security Applications Conference)

December 4-8, 1989

Westward Look Hotel, Tucson, Arizona

Sponsored by

IEEE Technical Committee on Privacy and Security

American Society for Industrial Security

Aerospace Computer Security Associates

### Conference Highlights

Keynote Speaker: Senator Dennis DeConcini (D - Arizona)

Luncheon Speakers: Mr. Charles. T. Force, NASA and Mr. Dave Fitzsimmons,  
Cartoonist, Arizona Daily Sun

Distinguished Lecture in Computer Security: "INFOSEC: Where Are We Going?",  
Stephen T. Walker, Trusted Information Systems

### Tutorial Program

Monday, 4 December 1989

"Secure System Design - An Introduction", Morrie Gasser, DEC

"Database Security", Teresa Lunt, SRI

Tuesday, 5 December 1989

"Secure System Design - Advanced", Virgil Gligor, University of Maryland

"A New Approach to Network Security", Jerome Lobel, Lobel Consulting

"Computer Crime", Ms. Gail Thackeray, Arizona Assistant Attorney General

Technical Program, Wednesday - Friday, 6-8 December 1989

### Technical Paper Sessions

- + Architecture for Trusted Systems
- + Network Security
- + Cryptographic Applications
- + Architecture and Mechanisms

- + Security Policy and Models
- + Risk Management
- + Software Development for Security
- + Data Base Security I & II
- + Security for Command and Control
- + Audit Applications
- + Trusted Distribution

#### Panel Sessions

- + Computer Crime
- + Data Base Design for MLS
- + TCB Subset Issues
- + Human Issues
- + Gemini Users
- + International INFOSEC Standards
- + Integrity
- + Shoot Out at the OSI Security Corral
- + Civil Sector Security
- + Security Standards for Open Systems
- + Space Station Information Security
- + Data Integrity and Security for Computer Aided Acquisition and Logistics Support (CALS)

#### Special Events

Biosphere II: a prototype of the Earth for the future, Sonora Desert Museum:  
living animals and plants of the Sonoran Desert Region

#### Additional Information

For a copy of the advance program, which includes rates, schedule, registration form, and special activities, contact:

Diana Akers, Publicity Chair, (703) 883-5907 akers%smiley@gateway.mitre.org  
Victoria Ashby, Co-Chair, (703) 883-6368 ashby%smiley@gateway.mitre.org  
The MITRE Corporation, 7525 Colshire Dr., McLean, VA 22102

For exhibit information, contact Robert D. Kovach, Exhibits Chair,  
(202) 453-1182, rkovach%nasamail@ames.arc.nasa.gov



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 9: Issue 32

Monday 16 October 1989

## Contents

- [Missed zero blamed for air crash](#)  
[Dave Horsfall](#)
- [Software reliance/software problems and the Stealth](#)  
[Marc Rotenberg](#)
- [Coping with the unexpected - Friday's stock plunge](#)  
[Steve Bellovin](#)
- [Re: latest stock market crash](#)  
[Olivier Crepin-Leblond](#)
- [Atlantis launch delay](#)  
[PGN](#)
- [Keeping up with the \[Indian\(a\)\] Joneses in elections](#)  
[PGN](#)
- [Friendly advice... \[Datacrime\]](#)  
[David Gursky](#)
- [Re: Synchronizing Clocks](#)  
[Brian Randell](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✉ Missed zero blamed for air crash

*Dave Horsfall* <[dave@stcns3.stc.oz.au](mailto:dave@stcns3.stc.oz.au)>

*Tue, 10 Oct 89 14:52:26 est*

Taken from "Computing Australia", 9th October:

``Missing zero blamed for air crash

Brazilian crash investigators have concluded that a data input error caused the Varig Boeing 737 disaster that killed 12 people last month. Pilot Cezar Augusto saved the lives of 54 passengers by ditching his aircraft in the Amazon jungle tree tops after running out of fuel.

An investigating team from Rio de Janeiro believe Captain Augusto miskeyed his computer-controlled flightpath on take-off, omitting the

first zero from his true course of "0270" when en route to Mexico. The computer navigation system directed the aircraft south instead of north without the crew realising until it was too late.

The findings have been slammed by the Brazilian Airline Pilots' Association which says the true fault lay in the computer. A spokesman for the association said it had evidence that a flight course computer print-out had detailed the wrong course. The association is calling for a re-examination of Rio de Janeiro Airport's flightpath-mapping system to check on its safety."

Dave Horsfall (VK2KFU), Alcatel STC Australia, dave@stcns3.stc.oz.AU  
dave%stcns3.stc.oz.AU@uunet.UU.NET, ...munnar!stcns3.stc.oz.AU!dave

---

### ✂ Software reliance/software problems and the Stealth

<mrotenberg@cdp.uucp>  
Tue, 10 Oct 89 17:23:33 -0700

The Washington Post has run an extraordinary three-part series on the development of the Stealth bomber and the subsequent political turmoil as the project faces increasing public scrutiny and Congressional skepticism. The article was written by Rick Atkinson and appears in the 10/8,10/9, and 10/10 issues of the Post.

These two paragraphs are from today's article:

. . .

"Because of the unique, three dimensional computer design system, Northrop felt confident enough to skip the usual step of building master tools for a bomber prototype; instead, AV 1 [Air Vehicle 1, the first B-2 off the production line] would be a full production plane built with the same 'hard tooling' used on the rest of the fleet. Boeing and Northrop tested internal aircraft systems, such as fuel and hydraulics, on huge 'Iron Birds' that resembled full-sized bombers with their skins peeled away. Beginning in 1985, navigation and avionics equipment was tested in the air of NKC-135 aircraft flying out of Edwards Air Force Base in the Mojave Desert.

"Northrop believed that it could reduce the number of construction man-hours from 3.5 million on the first bomber to 1 million on the 11th. New aircraft often are plagued with production gremlins; those hiding in AV 1 caused another six months of delay. A computer software miscalculation meant that electrical wiring had to be done over because the first set of wires was cut too short, according to a former Northrop executive; a pressurized line blew out and took two weeks to fix because it lay in an inaccessible cranny of the plane." ...

---

### ✂ Coping with the unexpected - Friday's stock plunge

smb@ulysses.att.com <smb@hector.att.com>

Sat, 14 Oct 89 18:40:32 EDT

The AP wire service provides financial page tables for many newspapers. As part of the process, they filter out trades that are more than 3% off of the current price. That didn't work on Friday, when the market plunged; they were forced to adjust their filters to accept 50% differences. The data was manually filtered before the weekend editions to eliminate trades that were "clearly reported incorrectly".

--Steve Bellovin

---

**RE: latest stock market crash**

Olivier Crepin-Leblond <zdee699@elm.cc.kcl.ac.uk>

Mon, 16 OCT 89 14:49:24 GMT

Could the current stock market crash have been initially triggered by a time-bomb type of virus, set to Friday the 13th ?

Olivier Crepin-Leblond, Computer Systems & Electronics,  
Electrical & Electronic Eng., King's College London, UK.

---

**Atlantis launch delay**

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

Mon, 16 Oct 1989 16:21:36 PDT

One of the shuttle Atlantis' engine computers was replaced (on Friday the 13th) and the new one (230 pounds and \$6M -- or about \$25,000 per pound) installed and checked out the next day. The launch is now scheduled for 17 October, a five-day delay. (A Federal appeals court may consider the challenge to last week's ruling that the launch can go on despite the risk of plutonium contamination in the case of an accident, the subject of the earlier case.)

---

**Keeping up with the [Indian(a)] Joneses in elections**

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

Mon, 16 Oct 1989 16:15:39 PDT

Indian computers and Japanese software are about to be used in the first computerized voting in India. The opposition party leaders launched a protest, being concerned about how easily the party in power could manipulate the elections. They cited Ronnie Dugger's New Yorker article (7 Oct 1988) noted in [RISKS-7.70](#) and 78, and displayed a list of some of the ways in which elections could be rigged electronically. [Source: NY Times, 15 Oct 1989, page 5.

Also noted by henry@garp.MIT.EDU (Henry Mensch).]

---

**Friendly advice... [Datacrime]**

David Gursky <dmg@lid.mitre.org>

Sat, 14 Oct 89 14:13:19 EDT

Once again, the voices of Light and Reason have triumphed over those of the Press. It seems that speculation of large amounts of data loss due to the Datacrime virus has been unfounded.

That being said, if you are not in the habit of backing up your computer's hard disk periodically, this would be a good time to start! Had Datacrime been widespread, and you had lost your system's hard disk's contents, where would you have recovered the information from?

Backups cannot *\*prevent\** malicious software from destroying or corrupting data stored on your computer's hard disk, but backups are *\*crucial\** to recovering the data lost to such an attack! There is an undeniable risk in believing that your computer is safe from malicious software simply because you practice safe computing. Our defenses are only as good as the problems we have seen. If tomorrow a vandal writes a new application to attack a computer system in a novel fashion, or a system that has not been subjected to many attacks, your data is as vulnerable as if you used no or minimal protection.

I am not trying to be an alarmist here, but the best strategy to safeguarding your data is a diversified one, and backups are a conerstone to any strategy.

And besides. Halloween is just over two weeks away.

---

## **✂ Re: Synchronizing Clocks**

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

Fri, 6 Oct 89 19:17:28 BST

In [RISKS 9.28](#) Earl Boebert suggested that a UK subscriber to RISKS might care to investigate whether the Synchronome Co. of Wembley, Middlesex, still existed. I have - to the extent of confirming that no company with the name and address he gave is now listed in the telephone directory.

I was motivated to investigate because of the problems we have with a master/slave clock system that is installed in building in which my office is located - though on checking I find that this identifies itself as having been made by "Gents of Leicester". The Gents system is in fact an appalling example of a good idea gone wrong. It was selected and installed by the University, I would guess about 25 years ago, with the aim of assisting avoidance of synchronisation errors in lecture start/stop times. Unfortunately, it now has exactly the opposite effect!

The problem is that individual slave clocks occasionally fail to receive, or react to, pulses from the master, and there is NO means of synchronising the slave clocks from the master. So, over a period of months, the various slave clocks gradually get further and further behind the master clock, and only get re-synchronised when a technician is sent to correct each of them manually - a job that in a building this size takes many hours if not days, and so is

performed only rarely, when many of the slave clocks are hopelessly slow.

The solution we have adopted in the Computing Laboratory has involved a unilateral declaration of independence from the central maintenance services. This is the replacement of those slave clocks which matter to us by ordinary quartz crystal-controlled wall clocks. These are quite cheap, far more dependable individually, and subject only to common mode failures which are likely to cause situations in which the clocks' accuracy is irrelevant, e.g. collapse of the whole building.

Brian Randell, Computing Laboratory, University of Newcastle upon Tyne  
JANET=Brian.Randell@uk.ac.newcastle UUCP=..!ukc!newcastle.ac.uk!Brian.Randell



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 9: Issue 33

Sunday 22 October 1989

## Contents

- [Earthquake preparedness in computing](#)  
[PGN](#)
- [Air-Traffic Disruptions](#)  
[PGN and Robert Dorsett](#)
- [Railroad Level-Crossing Monitoring](#)  
[Brian Randell](#)
- [Sometimes touch-screens aren't user-friendly](#)  
[Jeffrey Mogul](#)
- [UK Banking Error](#)  
[Brian Randell](#)
- [Quotron goes the bears and bares the bulls](#)  
[PGN](#)
- [Quotron software timing error](#)  
[David B. Benson](#)
- [Re: latest stock market crash](#)  
[David Gursky](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **Earthquake preparedness in computing**

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

Sun, 22 Oct 1989 12:35:32 PDT

Tuesday's Loma Prieta earthquake continues to have a devastating aftermath, particularly in parts of Santa Cruz, Hollister, San Francisco and Oakland. However, there have been some encouraging success stories of organizations with computer/communication contingency plans that worked successfully following Tuesday's earthquake (17 Oct 89). Furthermore, it appears that the area was spared much greater devastation because of anticipatory construction improvements.

The San Francisco Chronicle kept publishing despite a complete power outage at the newspaper's headquarters, which ground their computer and main printing facility to a halt. Material for the Wednesday and Thursday editions was

assembled using Macintosh disks and an emergency generator.

There was building damage at SRI. Most of the SRI Computer Science Lab computer facility survived. However, the RISKS file server was down until Thursday; when it was resurrected, the disk on which RISKS operates was discovered to be messed up as well, so I could not put an issue out until now.

---

### **✂ Air-Traffic Disruptions [with contributions from Robert Dorsett]**

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

*Sun, 22 Oct 1989 12:24:07 PDT*

For the second time in a week air traffic at Dallas-Forth Worth International Airport was disrupted. The Thursday 19 October computer outage (1950s-vintage computer system) lasted at least twelve hours, and caused delays. [Source: Washington Post, 21 Oct 89, p22]

FAA officials said Thursday's breakdown happened when one of four data processors on the computer failed to start after routine maintenance. The processors feed specific information about each plane from the radar to the controllers' screens. Flights continued at a reduced rate during the outage.

The previous week's outage, on 14 Oct 89, lasted for 19 minutes. It was traced to a technician who mistakenly tried to program a radar computer from the wrong terminal.

Tony Dresden, a spokesman for the National Association of Air Traffic Controllers, said the FAA is trying to upgrade computer systems across the country. But the process is painstakingly slow, he said. "I think if you go to any terminal across the country you'll find some older equipment mixed in with some new equipment," Dresden said. "So this is not just confined to terminals at the Dallas-Fort Worth airport, but to terminals across the country."

Norm Scroggins, tower manager at D-FW airport says the FAA is looking into the problem. "We're in an interim mode," Scroggins said. "I don't think it's particularly useful that any government agency is unable to stay up with the technological industry. It's just hard to get the stuff in. "And you have to keep in mind that this same equipment is working quite well in Houston. They just don't have the demands that we (D/FW) have."

[Excerpted by PGN from an article from the The Austin-American Statesman, 21 Oct 89, provided by Robert Dorsett (@rdd@rascal.ics.UTEXAS.EDU)]

---

### **✂ Railroad Level-Crossing Monitoring**

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

*Tue, 17 Oct 89 19:08:36 BST*

[This is interesting as an experiment in using AI - or more specifically neural networks - in a safety-related application, though not in any safety-critical fashion.]

## BR USES 'COMPUTER VISION' TO MONITOR LEVEL CROSSINGS

The Independent, 17 Oct 1989, by Mary Fagan, Technology Correspondent

British Rail will use computers to monitor level crossings to see if cars should be allowed to cross them, in an attempt to assess how artificial intelligence and 'computer vision' can be used more widely on the rail network. As part of a major experiment to be announced today, computers emulating the human brain will monitor the level crossings, deciding when it is safe to lower and raise gates, and when cars and pedestrians should be allowed to pass through.

Dr Alan Cribbens, head of safety systems at BR, said such systems would be used only to help and augment human control. But he hopes computer vision and artificial intelligence may also be used for examining the condition of rail tracks and tunnels, and for inspecting the conditions of the brakes on rolling stock. 'Computers would never be allowed to take decisions alone in the primary safety loop, at least not in the short term.'

Level crossings are currently monitored by closed-circuit television and controlled by an operator. There is a limit as to how many crossings one person can cope with, and the computer monitoring could dramatically increase the efficiency.

The experiment also acts as a tough test for computer vision, because it has to cope with variable lighting and weather, and to decide whether a scrap of paper or rubbish on the track constitutes a serious obstruction. The computer is a 'neural network' - a machine which attempts to emulate the way the brain works. The network is made up of layers of transputers, each of which is a computer in its own right, and which represent a computer neuron or brain cell.

According to Colin Hebden of SD, the company supplying the system, the neural network can be trained to recognise patterns and interpret images - things which traditional number-crunching machines are not good at. The transputer is also ideal because it communicates well with other transputers in the network.

The BR experiment is said to be pushing forward the frontiers of neural network computers. 'If it has potential we will have it in use as soon as possible,' Dr Cribbens said.

Brian Randell, Computing Laboratory, University of Newcastle upon Tyne  
JANET=Brian.Randell@uk.ac.newcastle UUCP=...!ukc!newcastle.ac.uk!Brian.Randell

[BR = British Rail, not Brian Randell.]

---

### ✂ Sometimes touch-screens aren't user-friendly

Jeffrey Mogul <mogul@decwrl.dec.com>  
20 Oct 1989 1741-PDT (Friday)

Last night I went into a hardware store (Builder's Emporium in Redwood City, CA) and walked past a kiosk providing advice from "Pop Larsen", probably a

fictional character. In addition to little brochures ("How to unclog drains") the kiosk contains a touch-screen system that apparently allows the user to navigate through some menus to get home-repair information.

What caught my eye was that, superimposed on the flashy 3d-ish color "buttons" on the screen, was a black & white message in a crude font:

Overflow in line 0 of module 1W4200YC at  
address 328F:0501

Hit any key to return to system

Of course, hitting "any key" was difficult, given that there were none.

-Jeff

---

## **# UK Banking Error**

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

*Fri, 20 Oct 89 12:53:44 BST*

[I have used the hash symbol (#) for the pounds symbol. I am assuming that the the story is using the term "billion" with its normal American meaning! Brian Randell]

### **BANK ERROR HANDS OUT #2BN IN HALF AN HOUR**

Computer Weekly, Thursday 19 October 1989, p.1, by Tony Collins,

A UK bank has accidentally transferred #2bn to UK and US companies because a software design flaw allowed payment instructions to be duplicated. The organisation has asked customers to return the money, which is more than the annual profits of any clearing bank, but so far not all of the cash has been recovered. The error, described by the Computing Services Association (CSA) as probably the most serious to have hit the IT industry, led to the #2bn being paid out to customers over 30 minutes.

Within an hour the bank discovered its mistake, but by then the cash had been transferred to other banks and into accounts of corporate customers in the UK and US. The funds were sent on the high-speed Clearing House Automated Payment System (Chaps) which allows high value payments, typically #2m, to be transferred in seconds from one bank to another via a computer system linked through British Telecom's Packet Switched Service.

Although Chaps refuses to name the bank it confirms that the accidental transferral of #2bn occurred "in the past few weeks" and involved one of its 14 member banks. The membership includes all major clearing banks together with the Bank of England, Girobank and the TSB. Jim Reeves, Chaps technical manager, says funds transferred on the network are guaranteed payments and are technically irretrievable. "If a bank decides it has made a mistake, it is still bound to settle the funds at the end of the day." He adds that, as far as he knows, most of the #2bn has been recovered as a result of the goodwill of the close-knit banking community and its corporate customers. "One bank

managed to send a number of payments it had sent the day before," says Reeves. "It only noticed this because of a very high outflow of money early in the day. It was a question of getting in touch with customers and asking them if they minded payment going back."

Richard Allen, chief executive of the Association for Payment Clearing Services (Apacs), which controls Chaps, says security and reliability have become increasingly important in payment mechanisms, especially as more institutions began using such systems. "This is particularly so in high value mechanisms such as Chaps," he says. Reeves says the \$2bn involved mostly foreign exchange and money market transactions.

The error was due to a software flaw which allowed the system to choose a date for payments rather than insisting that the operator made the selection.

In the event the system chose the wrong date.

The software has since been redesigned to avoid a repetition of the incident.

Brian Randell, Computing Laboratory, University of Newcastle upon Tyne  
JANET=Brian.Randell@uk.ac.newcastle UUCP=...!ukc!newcastle.ac.uk!Brian.Randell

---

### **✂ Quotron goes the bears and bares the bulls. Oxidentally.**

*Peter G. Neumann <NEUMANN@CSL.SRI.COM>*

*Tue 17 Oct 89 15:36:20-PST*

Following the wild drop on the NY Stock Exchange on Monday, Quotron reported at 10:30 AM on Tuesday, 17 October 1989, that the Dow Jones industrial average was DOWN 71 points. An unwitting NYSE VP announced this figure live on CNN, which caused quite a stir. However, almost all of the stocks (except the American and United Airlines companies) were UP, and the average should actually have been UP about 20 points.

Quotron gets live feeds from the market mainframes, and calculates the averages every 15 seconds. However, the heavy volume on the NYSE "overloaded" Quotron's software. The problem apparently corrected itself half an hour later.

"Nonetheless, the incident underscored how modern telecommunications have come to tie investors and markets together around the globe and the threats to market stability when the systems malfunction." (John Burgess, Washington Post, 17 October 1989)

---

### **✂ Quotron software timing error**

*David B. Benson <dbenson@cs2.cs.WSU.EDU>*

*Wed, 18 Oct 89 15:48:45 PDT*

Excerpts from:

Traders Who Can't Believe Their Eyes Win Vindication  
Heavy Stock Volume Makes Some of Quotron's Data Veer

Away From Reality

by Georgette Jasen,

Staff reporter of The Wall Street Journal

The Wall Street Journal, October 17, 1989, page c23

Traders ... were stunned to see the Dow Jones Industrial Average plummet 99 points in seconds. A minute later it soared 128 points, then zoomed back down 113 points, 69 below Friday's close.

...

Quotron Systems Inc., a Citicorp unit, blamed the 30-minute foul-up on "a timing problem in our software" caused by the enormous early volume -- about 145 million shares in the first hour of New York Stock Exchange trading. The prices of the individual stocks that make up the average were correct, Quotron said, but the average was wrong. ...

It was the second time in less than a week that Quotron has had problems calculating the industrial average. ...

[The earlier problem was attributed in a previous article to human error.]

A Quotron spokeswoman said recent software changes may have contributed to yesterday's problems. She said Quotron switched to a backup system until the problems were corrected.

---

## ✉ Re: latest stock market crash

David Gursky <dmg@lid.mitre.org>

Tue, 17 Oct 89 21:50:35 EDT

In [Risks 9.32](#), Olivier Crepin-Leblond <zdee699@elm.cc.kcl.ac.uk> asks if the 13 October 1989 drop in the average price of stocks on the New York Stock Exchange could have been triggered by electronic vandalism of some form (he specifically asks about a virus).

The possibility does exist, but (1) in this instance I do not believe that was the case and (2) if it were the case, we would know about it by now I should think.

Friday's plunge (as I understand it) was caused by preprogrammed selling of stock by computer. The rules and conditions under which these programs operate are well understood. If those programs had made transactions "outside of their envelope", the institutions that set the rules for the programs would be screaming bloody murder, and we would see the SEC all over the evening news.

Expanding this a bit, I find it less than likely (although I doubt it is impossible) for electronic vandalism (viruses, logic bombs, or time bombs) to effect these applications unnoticed. [I might add that when I say "less than likely", the basis of my comparison is the computing community in general, which is far more open than the NYSE's computers.] Again, preprogrammed trading occurs only under known conditions. It should be possible to put in some minimal amount of safeguards to prevent these automated trades to occur outside of their defined envelopes. This is not to say NYSE has done so though.



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

**Volume 9: Issue 34**

**Tuesday 24 October 1989**

## Contents

- [Earthquake and Computers](#)  
[Bill Murray](#)
- [Black Friday was only grey in Boston](#)  
[Pete Kaiser](#)
- [Human chess supremacy at risk?](#)  
[Bob Barger](#)
- [CERT Ultrix 3.0 Advisory](#)  
[Ed DeHart](#)
- [CERT DECnet Worm Advisory](#)  
[Ed DeHart](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **Earthquake and Computers**

<WHMurray.Catwalk@DOCKMASTER.NCSC.MIL>

Mon, 23 Oct 89 13:03 EDT

Today's ComputerWorld contained a number of articles on the impact of the 1989 San Francisco earthquake on computers. I thought the following note about the impact of computers on the earthquake was interesting.

"It is a measure of the dependence of a bank's customers that even after crossing a foot-wide crack in the sidewalk in the city's Mission District, one customer complained bitterly that the teller machine would not work. When reminded that the system's cables had to span the quake-torn area, the customer replied, "You'd think they'd know how to do something about this."

And, of course, they do. The answer is to have many ATMs. A nearby article reports that eighty percent of the cities ATMs were up and running.

William Hugh Murray, Fellow, Information System Security, Ernst & Young  
2000 National City Center Cleveland, Ohio 44114  
21 Locust Avenue, Suite 2D, New Canaan, Connecticut 06840

---

## ✂ Black Friday was only grey in Boston

*Mgr, Systems Consulting; 296-4345 <kaiser%cheese.DEC@src.dec.com>*

*Sun, 22 Oct 89 18:32:45 PDT*

While driving to work the Monday after the 190-point Friday-the-13th drop in the Dow Jones index, I heard on WBUR (public radio morning news in Boston) an interview with one of the managers of the Boston Stock Exchange, said in the program to be one of the fastest-growing in the United States.

He remarked that the Boston Exchange had no difficulty keeping up with the volume of trading nationwide, because their computer system could be turned off gracefully so that trades could be done manually -- apparently the only way to keep up with high volumes. (Remember all those stories of computers unable to keep up with the volume of trading?) He remarked further that the Boston exchange was able to keep up with the business on the day of the 500-point drop because the computer system wasn't yet installed.

Sounds very sensible to me, and though I'm tempted to editorial comment, I'll refrain.

---Pete

kaiser@cheese.enet.dec.com DEC, 2 Mt. Royal Ave. (UPO1-3), Marlboro MA 01752-9108  
508-480-4345 (machine: 617-641-3450)

---

## ✂ Human chess supremacy at risk?

*Bob Barger <CFRNB@ECNCDC.BITNET>*

*Mon, 23 Oct 89 11:01 CDT*

THE NEW YORK TIMES (National edition) for Monday, October 23, has a front-page story headlined "Kasparov Beats Chess Computer (for Now)." The story (written by Harold C. Schonberg) reports that Gary Kasparov, the highest-ranked player in the history of chess, beat a computer named "Deep Thought" in the first game of a two game match. Commenting on the prospect of a more powerful machine being developed in five years that could scan a billion chess positions a second, Mr. Kasparov was reported to have said: "That means I can be champion for five more years....But I can't visualize living with the knowledge that a computer is stronger than the human mind. I had to challenge Deep Thought for this match to protect the human race."

In many respects, a computer already is "stronger" than the human mind. Perhaps what Mr. Kasparov fears is that a computer might become more "creative" or "original" than the human mind...that it might become something more than an "extension" or "tool" of the human mind. Clearly, a lot of terms will have to be defined before that fear can be addressed...terms like "stronger," "creative," "original," "tool," "extension," and, perhaps most in need of definition, "human" and "mind."

Bob Barger, Eastern Illinois University

---

## **CERT Ultrix 3.0 Advisory**

<ecd@SEI.CMU.EDU>

Wed, 18 Oct 89 15:16:26 EDT

CERT Advisory Update  
October 18, 1989  
DEC/Ultrix 3.0 Systems

This is a repost of the Ultrix 3.0 advisory. We have received the sum output for DECstations.

=====  
Recently, the CERT/CC has been working with several Unix sites that have experienced breakins. Running tftpd, accounts with guessable passwords or no passwords, and known security holes not being patched have been the bulk of the problems.

The intruder, once in, gains root access and replaces key programs with ones that create log files which contain accounts and passwords in clear text. The intruder then returns and collects the file. By using accounts which are trusted on other systems the intruder then installs replacement programs which start logging.

There have been many postings about the problem from several other net users. In addition to looking for setuid root programs in users' home directories, hidden directories '.. ' (dot dot space space), and a modified telnet program, we have received two reports from Ultrix 3.0 sites that the intruders are replacing the /usr/bin/login program. The Ultrix security hole being used in these attacks is only found in Ultrix 3.0.

### Suggested steps:

- 1) Check for a bogus /usr/bin/login. The sum program should report the following for the DEC supplied login program.

```
27379 67 for VAXstation Ultrix 3.0
35559 116 for DECstation Ultrix 3.0
```

- 2) Check for a bogus /usr/etc/telnetd. The sum program should report the following for the DEC supplied telnetd program.

```
23552 47 for VAXstation Ultrix 3.0
45355 84 for DECstation Ultrix 3.0
```

- 3) Look for .savacct in either /usr/etc or in users' directories. This may be the file that the new login program creates. It could have a different name on your system.

- 4) Upgrade to Ultrix 3.1 ASAP.

- 5) Monitor accounts for users having passwords that can be found in the /usr/dict/words file or have simple passwords like a persons name or their account name.

- 6) Search through the file system for programs that are setuid root.

- 7) Disable or modify the tftpd program so that anonymous access to the file system is prevented.

If you find that a system that has been broken into, changing the password on the compromised account is not sufficient. The intruders do remove copies of the /etc/passwd file in order to break the remaining passwords. It is best to change all of the passwords at one time. This will prevent the intruders from using another account.

Please alert CERT if you do find a problem.

Thank you,  
Ed DeHart  
Computer Emergency Response Team  
Email: cert@sei.cmu.edu  
Telephone: 412-268-7090 (answers 24 hours a day)

---

### **✂ CERT DECnet Worm Advisory**

*<ecd@SEI.CMU.EDU>*

*Wed, 18 Oct 89 15:16:54 EDT*

CERT Advisory  
October 17, 1989  
"WANK" Worm On SPAN Network

On 16 October, the CERT received word from SPAN network control that a worm was attacking SPAN VAX/VMS systems. This worm affects only DEC VMS systems and is propagated via DECnet protocols, not TCP/IP protocols. If a VMS system had other network connections, the worm was not programmed to take advantage of those connections. The worm is very similar to last year's HI.COM (or Father Christmas) worm.

This is NOT A PRANK. Serious security holes are left open by this worm. The worm takes advantage of poor password management, modifies .com files, and spreads to other systems via DECnet.

It is also important to understand that someone in the future could launch this worm on any DECnet based network. Many copies of the virus have been mailed around. Anyone running a DECnet network should be warned.

R. Kevin Oberman from Lawrence Livermore National Labs reports:  
"This is a mean bug to kill and could have done a lot of damage. Since it notifies (by mail) someone of each successful penetration and leaves a trapdoor (the FIELD account), just killing the bug is not adequate. You must go in and make sure all accounts have passwords and that the passwords are not the same as the account name."

The CERT/CC also suggests checking every .com file on the system. The worm appends code to .com files which will reopen a security hole everytime

the program is executed.

An analysis of the worm appears below and is provided by R. Kevin Oberman of Lawrence Livermore National Laboratory. Included with the analysis is a DCL program that will block the current version of the worm. At least two versions of this worm exist and more may be created. This program should give you enough time to close up obvious security holes.

If you have any technical questions or have an infected system, please call the CERT/CC:

Computer Emergency Response Team  
Email: cert@sei.cmu.edu  
Telephone: 412-268-7090 (answers 24 hours a day)

=====

Report on the W.COM worm.  
R. Kevin Oberman  
Engineering Department  
Lawrence Livermore National Laboratory  
October 16, 1989

The following describes the action of the W.COM worm (currently based on the examination of the first two incarnations). The replication technique causes the code to be modified slightly which indicates the source of the attack and learned information.

All analysis was done with more haste than I care for, but I believe I have all of the basic facts correct.

First a description of the program:

1. The program assures that it is working in a directory to which the owner (itself) has full access (Read, Write,Execute, and Delete).
2. The program checks to see if another copy is still running. It looks for a process with the first 5 characters of "NETW\_". If such is found, it deletes itself (the file) and stops its process.

#### NOTE

A quick check for infection is to look for a process name starting with "NETW\_". This may be done with a SHOW PROCESS command.

3. The program then changes the default DECNET account password to a random string of at least 12 characters.
4. Information on the password used to access the system is mailed to the user GEMPAK on SPAN node 6.59. Some versions may have a different address.
5. The process changes its name to "NETW\_" followed by a random number.
6. It then checks to see if it has SYSNAM priv. If so, it defines the system announcement message to be the banner in the program:

W O R M S A G A I N S T N U C L E A R K I L L E R S



```

=====
$ Set Default SYS$MANAGER
$ Create BLOCK_WORM.COM
$ DECK/DOLLAR=END_BLOCK
$LOOP:
$ Set Process/Name=NETW_BLOCK
$ Wait 12:0
$ GoTo loop
END_BLOCK
$ Run/Input=SYS$MANAGER:BLOCK_WORM.COM/Error=NL:/Output=NL:/UIC=[1,4] -
  SYS$SYSTEM:LOGINOUT
=====

```

-----

Editor's note: This fix might only work if the worm is running as SYSTEM.

An earlier post made by the CERT/CC suggested the following:

```

$ Run SYS$SYSTEM:NCP
Clear Object Task All
^Z

```

You must then edit the file SYS\$MANAGER:STARTNET.COM, and add the line

```
CLEAR OBJECT TASK ALL
```

AFTER the line which says

```
SET KNOWN OBJECTS ALL
```

This has the side-effect of disabling users from executing any command procedure via DECnet that the system manager has not defined in the DECnet permanent database.

-----

2. Enable security auditing. The following command turns on the MINIMUM alarms. The log is very useful in detecting the effects of the virus left by the worm. It will catch the viruses modification of the UAF.

```
$ Set Audit/Alarm/Enable=(ACL,Authorization,Breakin=All,Logfailure=All)
```

3. Check for any account with NETWORK access available for blank passwords or passwords that are the same as the username. Change them!

4. If you are running VMS V5.x, get a copy of SYS\$UPDATE:NETCONFIG\_UPDATE.COM from any V5.2 system and run it. If you are running V4.x, change the username and password for the network object "FAL".

5. If you have been infected, it will be VERY obvious. Start checking the system for modifications to the FIELD account. Also, start scanning the system for the virus. Any file modified will contain the following line:

```
$ oldsyso=f$trnlnm("SYS$OUTPUT")
```

It may be in LOTS of command procedures. Until all copies of the virus are eliminated, the FIELD account may be changed again.

6. Once you are sure all of the holes are plugged, you might kill off NETW\_BLOCK. (And then again, maybe not.)



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 9: Issue 35

Wednesday 25 October 1989

## Contents

- [Offensive message on electronic information board](#)  
[Bob Morris](#)  
[John Crider](#)
- [14-year-old cracks TRW credit for major fraud](#)  
[Rodney Hoffman](#)
- [Foreplay Doesn't Effect Response Time](#)  
[Don Hopkins](#)
- ["Computer Virus Countermeasures" Article](#)  
[Will Martin](#)
- [Hardware failure mimics hackers](#)  
[Rob Wright](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **Offensive message on electronic information board**

<RMorris.CCS@DOCKMASTER.NCSC.MIL>

Wed, 25 Oct 89 12:52 EDT

Offensive Message Flashes at Busy City Corner

By Linda Wheeler

Washington Post, October 25, 1989

An offensive message that mystified the owners of an electronic information board was flashed Monday at Connecticut Avenue and L Street NW, one of the city's busiest intersections.

A Georgetown University law student, Craig Dean, said he saw the message "HELP STAMP OUT A.I.D.S. NOW: KILL ALL QUEERS AND JUNKIES" flash five times in 25 minutes. Minutes after seeing the message, he called the city Human Rights Office and the Washington Blade, a gay community newspaper.

Doug Hinckle, a staff photographer for the Blade, saw the message flash once and photographed it. ...

Judith Miller, president of Miller Companies, which own the building at 1101 Connecticut Ave. NW and the message board, said she did not know how the statement got onto the board. She refused to believe it had appeared until

told of the photographs.

Her company has complete control of the board and does not accept any paid messages or advertisements, Miller said. "I would never do anything like that," she said. "There is no way I would allow such a statement to appear."...

Yesterday, Keller, a five-year employee of the Miller Companies, said he did not write the statement and does now know how it became part of the normal flow of headline news.

Miller said she believes her computer system may have a "virus" and will have experts search to find where the unauthorized statement originated. "How absolutely awful," she said of the message. ...

[Also noted by John Crider, crider@itd.nrl.navy.mil, who added:

Possibly another case of how media-induced heightened awareness, this time about viruses, can lead to the emergence of a new scapegoat; years ago the operator would have been fired on the spot, but now it's a viral infection. Both are knee-jerk reactions - conclusions should come AFTER the facts are examined. -John Crider]

---

### ✦ 14-year-old cracks TRW credit for major fraud

Rodney Hoffman <Hoffman.ElSegundo@Xerox.com>  
25 Oct 89 09:02:23 PDT (Wednesday)

Condensed from a story by Jennifer Warren in the 'Los Angeles Times' 18-Oct-89:

A 14-year-old Fresno, CA boy obtained secret "access codes" to the files of TRW Credit from a bboard and used them to pose as a company or employer seeking a credit history on an individual whose name he picked randomly from the phone book. From the histories, he obtained credit card numbers which he then used to charge at least \$11,000 in mail-order merchandise (shipped to a rented storeroom) and make false applications for additional cards. He also shared his findings on bboards.

Police began investigating when TRW noticed an unusual number of credit check requests coming from a single source, later found to be the youth's home telephone number. The high school freshman, whose name was not released, was arrested at his home last week and later released to his parents. His computer was confiscated and he faces felony charges that amount to theft through the fraudulent use of a computer.

"Here's a 14-year-old boy with a \$200 computer in his bedroom ... and now he has shared his data with countless other hackers all over the nation," said Fresno Detective Frank Clark, who investigated the case. "The potential [for abuse of the information] is incredible."

---

### ✦ Foreplay Doesn't Effect Response Time

Don Hopkins <don@cs.UMD.EDU>  
Wed, 25 Oct 89 02:56:41 -0400

Computer Sex Game In Ambulance System (Associated Press)  
The Washington Post, Tuesday, October 25, 1987

NEW YORK, Oct. 23 -- A sex-oriented game is in the computer that monitors city ambulances, but an official dismissed speculation that the game could distract dispatchers or lead to computer problems.

John Petrofsky, a computer consultant for the Emergency Medical Services, said in the New York Post that "Foreplay" has been in the EMS system since September 1988. The program could slow the computer or stop it for 30 minutes, Petrofsky said. It also might carry a "virus" that could shut down the computer for two days, he said.

EMS spokeswoman Lynn Schulman said the inspector general of the Health and Hospitals Corp. had confirmed that the game was in the system, but she said it had no effect on response time, which has been reduced in recent months.

[Also indirected from Geoff Goodfellow]

---

### ✂ "Computer Virus Countermeasures" Article

Will Martin <wmartin@STL-06SIMA.ARMY.MIL>

Wed, 25 Oct 89 10:02:48 CDT

Readers of RISKS might be interested in a rather strange article in the October '89 issue of DEFENSE ELECTRONICS, p. 75, entitled "Computer Virus Countermeasures -- A New Type Of EW" [EW = Electronic Warfare], by Dr. Myron L. Cramer and Stephen R. Pratt (both of Booz, Allen & Hamilton, Inc.).

The reason I consider this "strange" is because the whole thrust of the article is how computer-based ECM [Electronic CounterMeasures] and EW systems could be infected by viruses which are transmitted over the air and enter those systems or their components via the normal sensing channels -- that is, they would pick up a digital stream the same way they would pick up an enemy radar signal, and that digital stream would contain code which would somehow find its way into the executable code for the system's processor(s). That whole concept seems very odd to me. Maybe I just don't know enough about the field to really understand this, but I cannot see how input data, which the system designers already know could be any electromagnetic signals or noise impinging on the system's sensors or antennae, could get intermixed with or interfere with the operating executable code of the sensor device or a central processor that is collecting and analyzing such data.

It is certainly obvious that an enemy agent working in or having access to the source of the software controlling such a computer-based EW system could implant a trojan horse or backdoor access into that software before it is fielded. Perhaps then the enemy could transmit a special sort of signal that would trigger the execution of such code in fielded systems, which would then self-destruct or provide erroneous results or otherwise misbehave. But I find it hard to envisage how some signals from outside, within the operational environment of such an EW system, could do anything to the executing code within embedded microprocessors or larger support computers. [Except of course

something like EMP or an electromagnetic-signal barrage that would just scramble the memories or damage the components of inadequately-shielded devices. But that would just render them inoperative, and would be the EW equivalent of blowing some holes in them. :-) It wouldn't surreptitiously install new code...]

The article does mention the idea of letting the enemy steal EW equipment or designs which have embedded in them trapdoor or other methods for allowing their functions to be subverted or controlled after they have been installed in enemy operational systems. I think this idea was used by Tom Clancy in *\_Cardinal of the Kremlin\_* or another of his books. Other methods mentioned include contaminating maintenance or diagnostic software with a virus. Those all seem fairly straightforward paths into executable software, but I still have problems trying to understand how sensed data could interfere with or modify executable code. Getting some virus program in the input data to go inside the operating code seems to me to be practically impossible, unless there is some sort of doorway or hole in that code that had previously been illicitly hidden there. It's sort of like the "blood-brain barrier" that makes it hard to deliver drugs into certain parts of the nervous system.

Is there something basic here I'm just not understanding, or is this article's basic premise flawed?

Regards, Will Martin

[Trapdoors abound. The sendmail debug option and the gets missing bounds check are recent reminders of the nature of the problem. Out-of-band signals also may trigger trapdoor effects. Furthermore, whether these effects result from an accidental flaw in the system or a preplanned Trojan horse program that would wait for the attack to be triggered, the results could be serious in either case. PGN]

---

### **✂ Hardware failure mimics hackers**

*"Rob Wright, VMS Systems Group, Curtin University" <CROBW@mail.cut.oz.au>  
Fri, 6 Oct 89 11:02 +8:00*

Dateline, Monday 20th September 1989, Bentley, Western Australia.  
Curtin University of Technology.

The VAX-11/750 computer in the Geophysics Laboratory refused to allow any user to log in. All passwords, including SYSTEM were declared invalid. The system manager contacted me and I showed him how to break in. There appeared to be some disk damage, but after setting all passwords to known values, the system was apparently usable. Shortly thereafter all was not well. Indeed, after any two users were logged in the system refused further logins, complaining that the licensed number of system users had been exceeded. Given that this particular machine (running VMS 4.7) has never been a microVAX, the only class of system which imposed such a limit, I naturally suspected foul play. At this stage I was sure that the system had been hacked, and was recommending a total re-installation of all the software, starting from known, reliable distribution tapes.

Then I read on the net that Columbia University Plasma Physics Laboratory has the very same set of symptoms and on the same date:-

>From: IVERS%CMR.MFENET@CCC.NMFECC.GOV  
>Subject:Virus or coincidence?  
>Date: 20 Sep 89 03:41:04 GMT  
>Message-ID:<890919204104.47800129@CCC.NMFECC.GOV>  
>  
>On Monday morning, our users (including the system manager) were surprised to  
>find that they could no longer log in to our VAX 11/750 (VMS V4.5).  
>Coincidentally, one user reported the appearance of several files in  
>his directory with names like WARNING., VIRUS., and ATTACK.. He thought  
>it was a joke and said nothing at the time the files appeared.  
>  
>The system was booted with UAFALTERNATE =1. It appeared that SYSUAF.DAT  
>was intact, but the passwords were no longer valid. A SYSUAF.DAT file  
>was restored from a backup set and new passwords were issued. The problem  
>is that now when more than 2 users attempt to use the system, a message  
>of the type LICENSED NUMBER OF SYSTEM USERS EXCEEDED appears.  
>  
>As for the "virus" files - all that remains are subdirectories of names  
>similar to the files reportedly seen by the user (one of them is called  
>[.DEADLY-VIRUS]).  
>  
>Any ideas as to the cause or cure of the LICENCED NUMBER OF... problem,  
>or insight into the nature of the "virus" would be appreciated.  
>  
>  
>                  Thanks in advance,  
>                  Tom Ivers (system manager)  
>                  Columbia U. Plasma Physics Lab  
>          Internet:  IVERS@CUPLVX.APNE.COLUMBIA.EDU  
>          MFEnet:   IVERS@CMR

My confidence in the hacking hypothesis rose by leaps and bounds. Then the advice starts to roll in:-

>From: coburn@clovax.enet.dec.com (John T. Coburn)  
>Subject:Re: Virus or coincidence?  
>Date: 20 Sep 89 23:25:20 GMT  
>Message-ID:<836@mountn.dec.com>  
>The LOGINOUT.EXE image in SYS\$SYSTEM would seem to be damaged, probably by the  
>virus attack that occurred. This may not be the only image damaged or changed.  
>You should restore the disk from a good backup tape. This is the only way you  
>can be sure of removing all artifacts of a virus attack.  
>A short term fix for the LICENSED NUMBER OF... problem is to get a good copy of  
>LOGINOUT.EXE off a backup tape (or your distribution tape VMS V4.4 - be sure to  
>check the V4.5 upgrade to see if it changed LOGINOUT.EXE).

>From: dragon@NSCVAX.PRINCETON.EDU (Richard B. Gilbert)  
>Subject:Re:Virus or coincidence?  
>Date: 21 Sep 89 00:57:49 GMT  
>Message-ID:<8909210036.AA10261@ucbvax.Berkeley.EDU>  
>  I think you've been well and truly screwed. The safest thing to do

>is to scrub your disk and restore from a backup that you are certain is  
>clean.  
>  
> I have this horrible feeling that SYSS\$SYSTEM:LOGINOUT.EXE has been  
>patched or replaced. Only extensive checking would reveal what else has  
>been tampered with. You had better assume that any sensitive information  
>on your system has been compromised and that anything may have been  
>tampered with!  
>  
> Even after you restore your system, you will still be vulnerable to  
>a repetition of the same attack! You will need to read and heed the "Guide  
>to VMS Security". You should probably have security alarm ACLs on  
>SYSS\$SYSTEM:SYSUAF.DAT, SYSS\$MANAGER:SYSTARTUP.COM or SYSTARTUP\_V5.COM,  
>SYSS\$MANAGER:SYLOGIN.COM and perhaps a couple of other things. This will  
>not prevent a breakin but it will make it tougher to do it tracelessly.  
>Check your modem lines if any. Are they all set /MODEM /HANGUP /DIALUP?  
>If not, they provide a potential entry point for a cracker.  
>  
> Priveleged accounts such as FIELD, and SYSTEST should be kept turned  
>off with /FLAGS=DISUSER and enabled only when needed.  
>  
> The default DECnet account also provides a potential point of entry.  
>  
> I'm real glad I'm not in your shoes.

>From: @YMIR.BITNET:KVC@FRIDAY.A-T.COM ("Kevin V. Carosso")  
>Subject:Re: Virus or coincidence?  
>Date: 21 Sep 89 00:57:00 GMT  
>Message-ID:<4EA69B97FB5FE04D85@YMIR.BITNET>  
>The fact that you are running VMS V4.5 and getting the "USERS EXCEEDED"  
>message is an important clue. User limits for MicroVMS were enforced by  
>code in LOGINOUT.EXE. When you upgraded your license on your MicroVAX,  
>say from 2 users to 8, DEC sent you a VMSINTAL kit which patched LOGINOUT."  
>  
>The fact that your 750 suddenly has a user limit of 2 (indeed any limit at all)  
>and is not running VMS V5 means that you may be running with a LOGINOUT.EXE  
>copied from a MicroVMS system. One distinct possibility is that someone  
>took the LOGINOUT.EXE from a MicroVMS system, possibly patched in their  
>own trapdoor, and copied it to your 750 replacing the standard  
>SYSS\$SYSTEM:LOGINOUT.EXE.  
>  
>A couple of years ago there were a rash of breakins to VMS machines  
>characterized, in part, by patched LOGINOUT.EXE's being left behind.  
>  
>You should consider restoring LOGINOUT.EXE from tape. You also might want  
>to save the suspicious one and check it out with ANALYZE/IMAGE (which will  
>report PATCH information unless the image was patched without using  
>the standard VMS PATCH utility).  
>

Finally Tom Ivers contacts me:-

>From: IN%"Thomas.Ivers%CUPLVX.APNE.COLUMBIA.EDU@munnari.OZ" 2-OCT-1989 10:53:09.83  
>To: CROBW@acad.cut.oz  
>CC:  
>Subj: Coincidence (not virus)  
>  
>Rob,  
> Our problems have been traced to a bad floating point accelerator in  
>our /750. Evidently, the virus files were a benign coincidence. You can  
>check this on your system by pulling your FPU and rebooting. (You'll have  
>to do a CONVERSATIONAL BOOTSTRAP because you'll find the passwords are mangled  
>after pulling the board). Otherwise, things should work fine without the FPU -  
>a bit slow, perhaps. Hope this helps.

Sure enough, when the FPA was replaced in our Geophysics machine the problems vanished. Apparently the FPA is used for password encryption. No one has satisfactorily explained the 'licensed users exceeded' phenomenon.

As to the failure mode of this subsystem, one presumes that those computing at the time of the failure would have some wrong answers, but further users were spared this worry by not being able to access the system.



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 9: Issue 36

Friday 27 October 1989

## Contents

- [Bug in Intel 486 chip](#)  
[PGN](#)
- [UK Banking Error](#)  
[Brian Randell](#)
- [The Presentation of Risky Information](#)  
[Joshua Levy](#)
- [Hardware failure mimics hackers](#)  
[Pat White](#)  
[Andy Goldstein](#)
- [Worms in a data stream](#)  
[Rick Simkin](#)
- [CERT Advisory on Sun RCP](#)  
[J. Paul Holbrook](#)
- [Warning About CERT Warnings](#)  
[anonymous](#)
- [Licensed users exceeded](#)  
[Tim Steele](#)
- [A lesson involving 'CRACKERS' \(APPLE II\)](#)  
[Olivier Crepin-Leblond](#)
- [Info on RISKS \(comp.risks\)](#)

---

### Bug in Intel 486 chip

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

Fri, 27 Oct 1989 10:41:03 PDT

This morning's San Francisco Chronicle notes that there is a flaw in the trigonometric functions in the new 486 chip. It was discovered by Compaq in testing its new system, expected to be announced on 6 November. New chips without the flaw will begin to appear next week, with volume production a few weeks away. This may delay some of the applications that are in the works.

The chip contains 1.2 million transistor equivalents, and at 12 to 15 MIPS is three times faster than the 386 chip. 200 companies are reportedly actively

designing new computers using the chip.

[Which chippies could talk about a better MOS TRAP  
with everyone making a beaten path to their door?]

---

## ✂ UK Banking Error

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

*Fri, 27 Oct 89 16:54:02 BST*

There has been a follow-up article in Computer Weekly (Oct 26, 1989, p.9) to the story about the software error which caused #(pounds)2 billion in duplicate payments, which I posted to RISKS (UK Banking Error, [RISKS 9.33](#)) last week. The new article, though quite lengthy, doesn't add much detail. However it does reveal that the bank concerned was Citibank, that 95% of the #2bn payments were reversed within the same day, that delays only occurred where Citibank was "acting through intermediaries or other branches", and that all the money was returned within three days.

The nicest bit in the new article is where it indicates that the story was originally broken in a speech by Jim Reeves, technical manager of the Clearing House Payment Systems (Chaps) to a gathering of bankers and other financial industry delegates at the Compsec computer security conference:

"Reeves struck observers as the most unlikely bean-spiller in the financial industry. His voice was so unexpressive that his Compsec speech left one immaculately dressed banker in the audience slumped across two seats, snoring loudly.

The enormity of the #2bn error was lost on his audience. Yet Reeves was saying, in effect, that in a matter of minutes a systems or operator error could cost a bank more than its annual profits."

And the article ends:

"Citibank insisted that there had been no financial loss to the bank or any third party as a result of the error. But this comment begs many questions which Citibank would not answer. What about the lost interest on the #2bn? Even a day's lost interest would amount to more than #500,000.

...

To most people the idea that systems could be so vulnerable as to allow a criminal, perhaps organised criminals, to divert electronically hundreds of millions into false accounts would be inconceivable - just as incredible as the notion that a bank could pay out #2bn by mistake."

Brian Randell, Computing Laboratory, University of Newcastle upon Tyne, UK

---

## ✂ The Presentation of Risky Information

Flame Bait <joshua@Atherton.COM>

Thu, 26 Oct 89 16:44:31 PDT

Background:

I have written a paper, "A Comparison of Commercial RPC Protocols" (RPC stands for Remote Procedure Call, and it is a simple way of writing distributed applications). This paper contained two sections: one comparing the speed of various RPC products, another comparing their reliability. This paper has been read by dozens (hundreds?) of people, and I have gotten a lot of feed back about it.

Problem:

The problem is that everyone ignores the reliability section of the paper. People are constantly discussing the relative speeds of the RPC systems, but they ignore the differing reliability measures.

I am in the process of writing the second version of this paper, and I want people to pay more attention to RPC reliability, but since I do not know why they ignored reliability in the first paper, I do not know what to change in the second paper.

Discussion:

In the first version of the paper the speed section came first and was longer than the reliability section (3 pages vs. 1 page). For the second version, I plan to put the reliability section first, and try to run more reliability tests. Unfortunately reliability is, in many ways, simpler than speed, so I doubt the reliability section will ever be as long as the speed section.

A second possible problem is that my wording was too neutral or too clinical, and that I should replace it with stronger or more emotional language.

I have a bad feeling that the reaction I am seeing is just a reflection of the fact that programmers and programming companies care much more about speed than reliability. I'm worried that no matter how I present the information, the reliability numbers will be ignored.

If you have any thoughts (answers or just comments) please email them to me, even if you send them to RISKS. (I do not seem to get every RISKS issue.) I will summarize responses sent to me. Tell me if you do not want your response summarized, or if you want to be anonymous. Thanks.

Availability:

The paper in question, comparing RPCs, is available by sending email to archive-server@joshua.atherton.com. The body of the message should contain the lines "send other comprpc.shar" or "send other comprpc.txt". The first line will give you the paper in troff's me macros, the second in plaintext.

Joshua Levy                    joshua@atherton.com    home: (415) 968-3718  
                                  {decwrl|sun|hpda}@athertn!joshua    work: (408) 734-9822

---

**🔥 Re: Hardware failure mimics hackers (Rob Wright, [RISKS-9.35](#))**

<ain@sage.cc.purdue.edu>

Fri, 27 Oct 89 12:38:37 -0500

>Sure enough, when the FPA was replaced in our Geophysics machine the problems  
>vanished. Apparently the FPA is used for password encryption. No one has  
>satisfactorily explained the 'licensed users exceeded' phenomenon.

If your FPA is like the one on our dual 780's, then it is also used to speed up integer math -- therefore, inode calculations and the like can be affected. Since file system damage was reported, this probably was the case. So, the 'licensed users exceeded' might be caused by the system looking at the wrong disk sectors.

>As to the failure mode of this subsystem, one presumes that those computing at  
>the time of the failure would have some wrong answers, but further users were  
>spared this worry by not being able to access the system.

Yup, they do get wrong answers... and sometimes even notice it (which is another computer "risk" -- people assuming that computers \*never\* make math mistakes).

Pat White

---

### **✂ RE: Hardware failure mimics hackers (Rob Wright)**

Andy Goldstein <goldstein%star.DEC@src.dec.com>

Wed, 25 Oct 89 15:08:02 PDT

A couple of points regarding the notes from Rob Wright and Tom Ivers regarding wholesale password failures and multi-user licensing problems caused by a faulty floating point accelerator:

- (1) The FPA implements integer multiply as well as the floating point operations, since a fast integer multiply helps array references often associated with floating-point intensive applications.
- (2) The Purdy algorithm [CACM, August 1974] VMS uses for one-way encryption of passwords makes extensive use of integer multiply operations.
- (3) The multi-user license validation algorithm used in VMS V4.\* also uses the Purdy algorithm in checking its license database.

Thus the bad FPA causes both user passwords and the multi-user licensing to fail. (Actually, a bad FPA can cause all sorts of things to fail because of the multiply implementation. Just another unfortunate consequence of an operating system's assumption that the CPU works.)

Andy Goldstein, VMS Development

---

### **✂ Worms in a data stream**

*Rick Simkin <simkin@zah.samsung.com>*

*Thu, 26 Oct 89 14:35:00 EDT*

In issue 9:35, Will Martin reported on an article which suggested that a data stream could somehow corrupt the workings of a computer system. He also expressed skepticism about this claim. From what I've heard recently, his skepticism is correct, as the claim itself is the product of confusion.

At a recent seminar hosted by the Greater Boston Chapter of the ACM, Pamela Kane and Andy Hopkins of Panda Software discussed this notion briefly. They cited a magazine article where someone had speculated that a spreadsheet overlay might contain malicious actions. Since spreadsheet files are commonly considered data, the Incautious Reader could jump to the conclusion that malicious data could take over a computer's operations.

Pamela Kane was quick to point out that a file which contained executable instructions--even if they were to be interpreted by another program, rather than run directly by the hardware--shouldn't rightly be considered a "data file."

Rick Simkin, Samsung Software America, Inc., 1 Corporate Drive, Andover MA 01810  
Any opinions expressed are my own, not my employer's.

[Don't forget the old squirreled-character mail message problem, where the normal reading of the mail message could trip up on a control character or escape sequence and cause a nasty effect. Just because it is data does not mean that it cannot somehow get executed... PGN]

---

### ***✂* CERT Advisory on Sun RCP**

*CERT Advisory <cert@cert.sei.cmu.edu>*

*Thu, 26 Oct 89 21:26:06 EDT*

CERT Advisory  
October 26, 1989  
Sun RCP vulnerability

A problem has been discovered in the SunOS 4.0.x rcp. If exploited, this problem can allow users of other trusted machines to execute root-privilege commands on a Sun via rcp.

This affects only SunOS 4.0.x systems; 3.5 systems are not affected.

A Sun running 4.0.x rcp can be exploited by any other trusted host listed in /etc/hosts.equiv or /.rhosts. Note that the other machine exploiting this hole does not have to be running Unix; this vulnerability can be exploited by a PC running PC/NFS, for example.

This bug will be fixed by Sun in version 4.1 (Sun Bug number 1017314), but for now the following workaround is suggested by Sun:

Change the 'nobody' /etc/passwd file entry from

```
nobody:*:-2:-2::/:
```

to

```
nobody:*:32767:32767:Mismatched NFS ID's:/nonexistant:/nosuchshell
```

If you need further information about this problem, please contact CERT by electronic mail or phone.

J. Paul Holbrook, Computer Emergency Response Team (CERT)  
Carnegie Mellon University, Software Engineering Institute  
Internet: <cert@SEI.CMU.EDU> (412) 268-7090 (24 hour hotline)

---

### **Warning About CERT Warnings**

<[Anonymous]>

Thu, 26 Oct 89 23:43:41 [x]DT

In [RISKS 9.34](#), CERT once again passes along advice on checking for security holes. Once again CERT recommends use of the UNIX utility "sum". Forgive me for shouting, but THE UTILITIES ON A POTENTIALLY COMPROMISED SYSTEM SHOULD NOT BE USED TO EVALUATE THAT SYSTEM'S SECURITY. This is especially true when CERT publishes the output the utility should produce. Another possibility is that a compromised file might be constructed in such a way as to produce the same output as an uncompromised file, even when viewed with an uncompromised utility.

A poor security procedure is worse than no procedure, because the poor procedure may produce a false sense of security. It's better not to know the truth and remain paranoid, than to know a false truth and feel comfy.

Sometimes I wonder whether CERT has been penetrated by a hacker.

---

### **Licensed users exceeded**

Tim Steele <tjfs@tadtec.uucp>

Thu, 26 Oct 89 09:51:39 BST

When I was using ULTRIX, we had the same problem after a system upgrade - the system would only allow 2 users to log in before reporting that the number of licenced users had been exceeded. Calling DEC confirmed this was the case, as they had just (in that release) installed a mechanism to check this. They promised they would ship us a tape to allow us to carry on using the system as before, but said it would take "several weeks".

I wasn't happy with this as we needed the system back online that morning (!) so I broke the protection system. Essentially it used a file in / (called /.license, I think) which contained 1K or so of "random" junk. This is the file you buy from DEC for a certain fee depending on how many users you want to enable on your system. The file gets opened by /etc/init and the number of licensed users read out and checked for every time a new login process is

started. This number is also printed at boot time.

GOTCHA: The number printed is NOT the same as the number used in the check! For a "real" license shipped by DEC, these numbers will be the same. The idea is to stop crackers disassembling init and patching the obvious number printed at startup. The real number is stored in several places in a suitably tricky way. Even so, armed with a couple of genuine licence files, it's fairly easy to crack. I ended up with a 10-lines-of-C utility that would forge any licence you liked...

If init reckoned the license was not valid, it would default to the minimum, i.e. 2 users. I suspect the VMS mechanism is similar, and is defaulting to 2 users as the value returned from the (bad) FPA is not matching the proper encrypted value in the system license.

---

### **✂ A lesson involving 'CRACKERS' (APPLE II)**

*Olivier Crepin-Leblond <ZDEE699@elm.cc.kcl.ac.uk>*

*Thu, 26 OCT 89 18:43:52 GMT*

This message is being sent to both RISKS and VIRUS lists. Apologies to those who receive both digests.

I was well shocked in finding-out that there was actually a virus running on the Apple II family of computers ! Where could the LODE RUNNER virus have infected such a small machine, with no integrated hard disk, and the possibility of rebooting the machine quickly by using a simple sequence of control codes ? (open-apple-ctrl- reset ). In FRANCE, of course !

The Apple II did very well in France. It is very widely used over there. This success, like in the U.S.A., triggered a large market for pirated copies of programs.

I have been an Apple II owner since 1982. It is absolutely amazing how many copies of programs went around since that time. I guess that virtually every program for this type of computer was available as a pirated copy in France. This is because of the following:

1. There are laws about unlawful software copying, but they are very hard to enforce. In addition to that, it is extremely difficult to find the originators of the software. ie: The "top" pirates are well hidden, and if the police was to catch every person who copies a program, then they'd probably have to prosecute virtually \*any\* computer user !
2. Most software was copied and "exchanged" against other software, a bit like a one to one swap. Commercial pirate factories were discovered in Lyons a few years ago. There, the programs were deprotected, copied, and then protected again, and sold to customers for a fraction of the price. The pirates were arrested and heavily fined (and given a prison sentence).

### **SOME SORT OF COMPETITION**

There were many independent groups of pirates. The average age was

16-22 years old. All of them were experts at Apple II's Disk Operating System. The most "advanced" of these "crackers" were the CCB. CCB for "Clean Crack Band". From the number of programs that they have cracked, they seemed to spend their days and nights cracking games and software. Some French magazines and newspapers wrote articles and interviews with them. They even went on national French TV. Of course, they were in hiding; a bit like drug dealers, really. The quality of their "work" was unbelievable. The program was as good as new, only it had their name in the presentation page. Often, they added pretty graphics, and additional options in some cases. In fact, it looked as though they had completely re-written the program entirely. At the end of 1985, I think, they renamed themselves, the SHC, "Solex Hack Band". (A Solex used to be a cheap moped at the time) They hacked a few French Computers by using dial lines; they did one "Hacking" direct, on TV, showing the journalists how vulnerable computers were. Since that time, I don't know what happened to them.

#### OTHER GROUPS

There are a lot of other groups of pirates around France. The CCB were based in Paris (according to the press), and the two most famous members of this group called themselves: Aldo Reset, and Laurent Rueil. Other groups include:

- Johnny Diskette: this name was used by many anonymous pirates who had formed some kind of club in Paris, where they had competitions (!) on who would be the fastest to unprotect a disk.
- BCG (Baby Crack Gang): funny name. They seemed to like Karateka games.
- CES (Cracking Elite Software): They added features to games from time to time.
- Chip Select and the Softman: These pirates went as far as including a digitised picture of themselves wearing dark glasses and saying: "I am Chip Select". A Certain Eric IRQ (Interrupt Request) was also part of this group.
- Mister Z (Geneva): These were Swiss pirates, but for some reason, they were sending copies to French crackers, telling them to change the title page that they had made-up. It was some kind of competition of: "We can protect this program; can you unprotect it ?"
- MAC (Marseilles Association of Crackers): group based in Marseilles.
- P.Avenue Nice: and this one is in Nice...

These groups deprotect the software. Once deprotected, it can be copied very easily using a normal copy program.

Most copying goes-on in large computer centres, where machines can be used free of charge. There is no supervision there, and no control on what goes-on. Some places are popular just because it is such an easy way to get hold of any program for no charge (well... just the cost of a diskette). Since 1987, though, the shops are more careful since they could be held responsible for what happens on their machines.

#### HIDDEN INFO

If you use a track/sector disassembler, you can see the information on the tracks of the disk displayed as ASCII characters. Often crackers would

converse between themselves in this way. Software is copied through a string of intermediaries, and the messages can therefore be passed this way. It is impossible to know if there is some hidden information on the disk if it is not analysed by using a track/sector disassembler. It is therefore very easy to hide other programs within the disk, whether they are games, or even viruses !

#### IN CONCLUSION

So in fact, considering the level of expertise that these crackers have, it would be very easy for them to hide a virus within a floppy disk, which would be triggered by the actual program. I am talking here about the APPLE II computer, but I am sure that other computers (including PC's) have their "expert" crackers, who no doubt, would be very happy to write viruses/worms/trojan horses/time bombs etc.

Why do they do it ?

My idea is that they do it for "fame", just to see other people talk about "their" virus. Any suggestions ?

Olivier Crepin-Leblond, Computer Systems & Electronics,  
Electrical & Electronic Eng., King's College London

Disclaimer: My own views. Any comments/flames/congratulations welcome !



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

**Volume 9: Issue 37**

**Sunday 29 October 1989**

## Contents

- [Low-tech wins the day in airliner mishap](#)  
[Glenn Story](#)
- [Hi-tech loses in cars](#)  
[Alayne McGregor](#)
- [Re: Hardware failure mimics hackers](#)  
[Sukumar Rathnam](#)
- [Re: Black Friday in Boston and manual systems](#)  
[D. W. James](#)
- [Re: Human chess supremacy at risk?](#)  
[Andrew Klossner](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **✉ Low-tech wins the day in airliner mishap**

<STORY\_GLENN#TSII@comm.tandem.com>

27 Oct 89 11:50:00 -0700

The following is copied from our internal "humor" distribution list, condensed from Flight International:

A DC9 with 104 people aboard made an emergency landing in Colorado last week. The aircraft, Northwest flight 109 from Minneapolis to Phoenix diverted to Monte Vista municipal airport after losing both generators and the auxiliary power unit in mid-air.

The aircraft landed safely on the 1,830m runway, with no injuries, although it overran the runway by about 300m. The airline says the captain was forced to use an axe to open the forward cabin door, after the cabin began to fill with smoke. After evacuating the passengers, the captain then had to walk to the terminal and use a payphone to summon help.

Glenn Story, Tandem Computers

---

## **Hi-tech loses in cars**

*Alayne McGregor <alayne@gandalf.UUCP>*

*Thu, 26 Oct 89 00:45:40 EDT*

Car gadgets overwhelm, expert says (by Mary Gooderham)  
(Toronto Globe and Mail, Sept. 14, 1989)

Car drivers are being overwhelmed with technology that could endanger lives, a conference was told yesterday. Car telephones, facsimile machines, computers and navigation systems that can even allow drivers to check the menus of restaurants are providing more information than people can handle, Alison Smiley, an expert in the field of human factors, told the Vehicle Navigation and Information Systems conference in Toronto. "High technology hasn't added anything to safety and efficiency, it's detracted from it," said Ms. Smiley, head of Human Factors North Inc., a Toronto consulting firm. "The potential for providing people with information in the car is limitless," she said, adding that the capability exists to give drivers tips on the closest Chinese restaurant and its menu. "You don't want people to do some things while they're driving."

Since the early 1980s, the automobile and the computer have become increasingly integrated. Today, cars are being equipped with "head-up displays" (HUD) that project speed readouts before a driver's eyes while he looks through the windshield and video screens that display maps that tell drivers where they are and help them get where they are going.

The navigation systems, which would eventually be linked to "smart" systems to give drivers information about current road conditions, are already being produced by a California company, Etak Inc. Etak manufactures a device for keeping track of car movements: a map is displayed on a video screen and updated frequently as the car moves, showing the driver where he is and giving him the ability to get information about approaching features.

Ms. Smiley said three areas of limitations must be considered when designing such products: physical problems, a driver's perception of the instruments, and cognitive problems relating to how the information is processed. She said the main problem with communication and information in the car and HUD readout is that it distracts the driver.

One delegate told the conference that navigation displays require more, not fewer skills than a traditional printed city map, especially if the driver is unfamiliar with the area.

Acceptance of the systems may also be limited by its cost -- \$1,500 to \$3,000 (U.S.)

[This reminds me of a) a recent accident report in which a woman was killed: she didn't see a turn because she was putting on mascara, and b) the fact that my father would not even have a radio in the family car because he felt it stole a driver's attention away from \*driving\*.

Alayne McGregor ]

**✂ Re: Hardware failure mimics hackers ([RISKS-9.35](#))**

*Sukumar Rathnam <sukumar@emx.utexas.edu>*

*Sun, 29 Oct 89 11:35:54 -0600*

Continuing with the problems of the FPA on a VAX 11/750.... I once used a machine which had a FPA attached. Unfortunately the building the machine was in had an air-conditioner that was subject to FREQUENT breakdowns.

What used to happen was that if the temperature fell below a critical value the FPA would shut itself off. The rest of the machine did not know that the FPA was off. As a result any program that used the FPA would behave weirdly (in my case a graphics program IGL/PLOT10) but programs which did not worked just fine.

This was discovered when programs known to be correct would arbitrarily crash when the temperature was high but work fine when the ac was ok.

The last thing you expect is a temperature sensitive behavior for programs. Have people encountered similar problems or has the bug been fixed?

Sukumar Rathnam, MSIS Dept., CBA 5.202, The University Of Texas, Austin TX 78712

---

**✂ Re: Black Friday in Boston and manual systems ([RISKS-9.34](#))**

*D. W. James <vnend@phoenix.princeton.edu>*

*25 Oct 89 20:36:58 GMT*

In [RISKS Vol 9 Issue 34](#) kaiser%cheese.DEC@src.dec.com reported that the Boston Stock Exchange had little problem during the 10/13 stock crash, since the exchange had the capability to return to (faster) manual transaction handling. For me, this is believable.

I worked for several years in hotel work, auditing and front desk work mainly. At a couple of sites I worked with computerized desks and experienced the advantages and disadvantages of them. The biggest single disadvantage was at checkin, where being forced to rely on the computer to find rooms slowed check-in down to as little as one fifth the capacity I could handle manually. Eventually the manual system was reinstalled as a backup, and fast check-in speeds were again available... At the cost of more work, as the check-in information still had to be typed into the computer.

So, while I can easily believe that the BSE could handle manually more transactions than they could by computer, I'm also sure that there was also some overtime that evening/night as the computers were brought up to date...

Vnend

---

**✂ Re: Human chess supremacy at risk?**

*Andrew Klossner <andrew@frip.wv.tek.com>*

*Wed, 25 Oct 89 12:51:16 PDT*

There's an excellent article on the Deep Thought - Kasparov chess match in the 24.Oct.89 issue of the Wall Street Journal (page A16). It analyzes the development of the two games and the strategies involved. Apparently Kasparov studied Deep Thought's games and developed strategies to blow the computer out of the water, such as diverging early from established play patterns to get out of the computer's "book".

-- Andrew Klossner



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 9: Issue 38

Tuesday 31 October 1989

## Contents

- [Passwords in the Electronic Home](#)  
[Gary McClelland](#)
- [A new excuse](#)  
[Ernest H. Robl](#)
- [Hot computers and temperature-sensitive programs](#)  
[Donald Arseneau](#)
- [Re: Hi-tech loses in cars](#)  
[Paul Fuqua](#)
- [Article on computer crime laws](#)  
[Peter Ladkin](#)
- [Work processes which are done faster by hand than by machine](#)  
[Alexis Rosen](#)
- [Info on RISKS \(comp.risks\)](#)

---

### Passwords in the Electronic Home

"Gary McClelland" <[gmcclella@clpr.colorado.edu](mailto:gmcclella@clpr.colorado.edu)>  
31 Oct 89 11:55:00 MDT

As various electronic services are brought by phone lines or cables directly to the home, there will be an increasing need for folks to deal with passwords. And concomitantly there will be ever more lists of passwords for the nefarious to try to crack. RISKS readers may be interested in the following stories about passwords for two electronic services that recently arrived over the wires at my house. From the aspect of security, one story is good and the other bad.

1. Voice Mail. The local Bell company is offering electronic voice mail from the central switch to residential customers. Many advantages over an answering machine. Not only are both capacity and reliability better than for tape machine but there are also some nice features that an answering machine could not have such as answer when busy and a differential ring that lets the caller know he or she is being switched to voice mail with enough warning that he or she can hang up to avoid toll charges. The good story: on first use the

system requires you to enter a password (min 4 digits, max 8 digits) of your own choosing. In contrast, my old answering machine had a 1 digit security [sic] code. The password is also easily changed. I wish my multiple ATM cards would let me choose my own passwords so that maybe I could remember some of them.

2. PRODIGY. IBM and Sears have teamed to offer a modem-accessible information and shopping service. I think we are a test market but maybe lots of you have this available. Slick, but slow, graphics, available in either IBM-PC or Mac versions, offer information on sports, weather, etc. and, depending on locale, home banking, grocery shopping, and catalog shopping from places ranging from Sears and Penneys to REI. One particularly nice feature is access to American Airlines' Sabre reservations system through a front-end that although is sometimes tedious is much easier to use than a terminal in a travel agency. This week I received a promotional letter from AA proffering goodies if I booked my own flights and paid for them with a credit card through Sabre. And just in case I had forgotten my password (which they told me never to write down) they had \*printed\* it at the top of the promotional letter! That clearly means they don't encrypt the passwords they collected from all of us (oh, they also have our credit card numbers and frequent flyer numbers for faster ticket ordering). I wonder how many AA people have access to the password list? Certainly everyone in the mail room! But if someone uses my password and credit card number to order tickets, will I at least get credited for the frequent flyer miles for the flights they steal?

Gary McClelland, Univ of Colorado

BITNET: mcllella@colorado

---

### **✂ A new excuse**

*Ernest H. Robl <ehr@uncecs.edu>*

*Tue, 31 Oct 89 14:50:34 EST*

From a conversation overheard a few days ago at the Duke University student center -- yes, this is real; I'm not clever enough to make up something like this -- a new version of the "my dog ate the homework" excuse for not getting a project done:

"I told the professor that with the medication I was taking it wasn't advisable for me to drive a car, operate heavy machinery, OR FORMAT FLOPPY DISKS."

My opinions are my own and probably not IBM-compatible.--ehr  
Ernest H. Robl (ehr@ecsvax) (919) 684-6269 w; (919) 286-3845 h  
Systems Specialist (Tandem System Manager), Library Systems,  
027 Perkins Library, Duke University, Durham, NC 27706 U.S.A.

---

### **✂ Hot computers and temperature-sensitive programs**

*<Donald\_Arseneau@mtsg.ubc.ca>*

*Tue, 31 Oct 89 05:51:34 PST*

In [risks 9.37](#) Sukumar Rathnam writes

The last thing you expect is a temperature sensitive behavior for programs.

Actually, I've seen it many times and it is now one of the first things I expect. And it's easy to test--just turn down the thermostat.

Donald Arseneau

---

✂ **Re: Hi-tech loses in cars (Alayne McGregor, [RISKS-9.37](#))**

Paul Fuqua <pf@islington-terrace.csc.ti.com>

Tue, 31 Oct 89 14:29:23 CST

Etak manufactures a device for keeping track of car movements: a map is displayed on a video screen and updated frequently as the car moves, showing the driver where he is and giving him the ability to get information about approaching features.

Nicholas Negroponete of the MIT Media Lab used this very application as an example of the need for speech interfaces to computers. In his opinion, it's a terrible idea to have a separate map screen that requires the driver to take his eyes off the road. It's much better for the map to talk to him: "Turn left at Elm Street, 1/4 mile ahead." Even a heads-up display isn't good enough -- don't overload one channel of communication, use two channels that don't overlap.

Paul Fuqua, Texas Instruments Computer Science Center  
pf@csc.ti.com {smu,texsun,cs.utexas.edu,rice}!ti-csl!pf

---

✂ **Article on computer crime laws**

Peter Ladkin <ladkin@icsib.Berkeley.EDU>

Mon, 30 Oct 89 13:15:49 PST

This week's Economist (28 oct - 3 nov issue) has a leader article on computer crime (p18), saying that the rush to define new laws on computer crime is leading to inappropriate suggestions for punishment. They say the 'real menaces' are not mysterious or new, but 'old-fashioned trespass, vandalism and theft', and that laws against the former two are hard to apply because 'the "space" and "property" inside a computer are intangible'. They point out two nonsenses that have been created by the proposal of Britain's Law Commission, note that extra-territoriality is a special problem posed by computer crime, and suggest (platitudinously) that the basic issue of how to protect (rather than how to punish) needs to be addressed further. In the usual Economist style, it is well-written and coherent, apart from the conclusion, which is hardly that.

I don't have a scanner, and am unwilling to type it all in. Copies should hit the bookstores wednesday.

---

## ✂ Work processes which are done faster by hand than by machine

Alexis Rosen <alexis@panix.UUCP>

Mon, 30 Oct 89 04:03:27 EST

I'm a newcomer to risks (not the net) but I've followed the discussion of slow computer vs. fast manual systems. This is a subject which I've some familiarity with, and right now I'm just finishing the installation of a very high-volume POS (point of sale) system implemented on (can you believe it?) a network of Macintoshes, with receipt printers, cash drawers, and bar-code scanners.

I have done other systems before which demanded speed, but this job was the most interesting and difficult I have faced. From it I have learned a number of things about the speed that can be achieved with computer systems in the face of real-world problems.

Problem #1: Careless and unintelligent employees.

Many employees, especially in the kinds of positions that wind up being automated (cashiers, tellers, etc.) are somewhat less than brilliant. If they were smarter they'd be rocket scientists, right? :-). There are many who are not dumb, and they can be worse, because boredom can make them incredibly careless.

Solution: Management has to be involved in maintaining a decent workplace, but there are still many things you can do to keep new technology from adding to the trouble (which would exist no matter what). I followed the "spirit" of the Mac interface, which really just means being aware of human factors- I could not use a mouse \*at all\*, so goodbye menus and icons. In general, everything has to be 100% bulletproofed and idiotproofed. These are not the same thing at all- one protects against illegal values completely, while the other warns against (but usually doesn't forbid) stupid values.

Example: After a couple of days, employees become aware of the general flow of events in the program, so they stopped looking at the messages for them on the screen- in fact they often didn't look at all. They were often unaware of conditions that required immediate action (bad price entered, for example). One solution to this particular problem was to create three distinct sounds that notified users of acknowledgement, notification, and error conditions.

Problem #2: Forgotten Features (and other training issues)

If the system can do so much, how come it's used for so little? Because nobody remembers how to do this, that, and the other thing. So they all do this instead of that and simply keep paper notes, or figure out some other way to do less work and screw up the system. Don't fight it, because you'll lose.

Solution: Make sure everything is accessible. Write software that requires a minimum of training. You want specifics? Start with the Apple Human Interface Guidelines, and then there's lots of other literature. But to begin with, don't hide features, don't use cryptic codes when simple english will do, and don't expect your users to know what they're doing- literally. Either tell them where they are at all times (unobtrusively, of course) or failing that,

allow them to back out gracefully. \*\*\* BE CONSISTENT \*\*\* and don't expect users to be the same.

Example: My POS system replaces standard cash registers. It does much much more and yet takes one-quarter the time to learn. And the features aren't forgotten. One Mac-ish thing it does is use title bars on all of the windows which aren't instant-response windows (modal dialogs). The title bars say who is logged in and what they're doing at all times.

Problem #3: Slow and/or increased data entry

Many computer systems require the tracking of much more information than the old manual systems. This can create the illusion of lethargic system speed even if the hardware is quite fast. Users can be frustrated by the extra load, which may well feel like makework to them. The speed of entry itself may be slow if data is validated on-the-fly as it's entered.

Solution: First, tune the software. You can achieve remarkable things by using (or, unhappily more often, faking) multi-threading -- do the validation, but don't stop data entry while you're validating. Overlap various hard delays- print while you're writing to disk, or calculate while verifying a credit number with a remote machine.

After all this helps, but isn't good enough, start buying hardware. This may well be the best part of the system to invest in. Special data-entry hardware can make a huge difference.

Example: After tuning the POS software, there was still an inevitable slowdown since the cashiers were entering price and item information instead of just the price (as on the old registers). This was costing up to fifteen seconds per item, which was completely intolerable. The solution was to buy bar-code scanners, which could enter both item # and price (both of which are typically on the item to begin with). This dramatically improves the performance of the item-entry process.

Problem #4: Lazy programming.

Yes, I am as lazy as the next guy. Often, I'd like the real world to fit a neat conceptual model I have developed for it. When a case comes up that I can't handle, I'd rather contort it to fit my code rather than the other way around. Sometimes this is feasible, and once in a while, it can lead to marked improvements- but if so, it just identifies an improvement that should have been realized earlier in the design process. Most of the time, shoehorning real procedures into flowcharts is a recipe for disaster.

Solution: In that case, recode. It's as simple and as painful as that. Sometimes you'll wind up with pages and pages of code to deal with a handful of exceptions that won't come up but once a year. Tough luck- that's what being a good programmer is all about.

Example: I designed the POS system so that every item sold would already be in the database. I went to great lengths to insure this, since it would make life much easier for both myself and all of the users. Unfortunately this can't always work- at times items may be checked in with faulty item codes, for example. Modifying the system to deal with unexpected item codes was one of the most annoying and inelegant things I have ever had to do, but now it works, and people no longer complain about having to work around a system

which is supposed to make their work easier, not harder.

There is more, but I think that this is more than enough for my first risks posting. The point of this is that the system I built is not only more capable and useful than the old, but is considerably more efficient up front, as well. I think that this achievement could easily be duplicated elsewhere if programmers were more aware of the real-life processes they are trying to model, and the real-life problems their systems will have to deal with.

Alexis Rosen, President, Arete Corp. (Hat #1)  
Sysadmin/Owner, PANIX public access Unix (Hat #2)  
cmcl2!panix!alexis -or- alexis@panix.uucp



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 9: Issue 39

Tuesday 7 November 1989

## Contents

- [Computer used to find scoflaws in Boston](#)  
[Barry C. Nelson](#)
- [Air Traffic in Leesburg VA](#)  
[PGN](#)
- [Equinox TV Documentary on "Fly By Wire"](#)  
[Brian Randell](#)
- [Lifethreatening risk! \(related to Soviet PCs\)](#)  
[Julian Thomas](#)
- [New computer risk: child abuse data base proposed \(W. K. Bill\) Gorman](#)
- [Dangers of mail aliases](#)  
[Jonathan Leech](#)
- [Committee report on Bugs](#)  
[Bob Morris](#)
- [Computer Viruses Attack China](#)  
[Yoshio Oyanagi](#)
- [First Virus Attack on Macs in Japan](#)  
[Yoshio Oyanagi](#)
- [NTT Challenges Hackers](#)  
[Mark H. W.](#)
- [Even COBOL programmers need to know about range checking.](#)  
[Bryce Nesbitt](#)
- [Unix Expo Power Failure](#)  
[Jan I Wolitzky](#)
- [Info on RISKS \(comp.risks\)](#)

---

### Computer used to find scoflaws in Boston

"Barry C. Nelson" <[bnelson@ccb.bbn.com](mailto:bnelson@ccb.bbn.com)>  
Sun, 5 Nov 89 13:14:43 EST

A news article in the Boston Globe [last Sunday 29 October, with photo] describes a new computer system, named Argus (after a mythical multi-eyed and vigilant beast), which is being used to catch local drivers with stolen license

plates. The innovation is that a sensor is used to observe license plates and a program turns the image into numbers (so they claim). A database is then searched and a match signalled to the operator. The system is set up at a toll booth at the harbor tunnel and the suspect is somehow pulled over by the State Police at the other end as the car emerges.

The article goes on to quote the operators as saying they have proven the system "works" by matching on six offenders in one day. Unfortunately, five of the six were errors caused by Registry backlog or other policy inconsistencies such as re-using old numbers for new car owners. The sixth case was bona fide.

Their current experiment uses one camera and a floppy database of some 40,000 registrations. They say they are looking forward to installing the list of 200,000 suspended licenses or registrations and increasing the number of cameras to enable them to watch all eight lanes.

When five out of six hits are human errors, imagine the complaints! It can be very humiliating to be hauled out of your car and treated like a felon. This could turn out to be embarrassing for the overworked database managers.

At least we can look forward to less tunnel traffic someday as Argus evaders find alternate routes.

BCNelson                    "Opinions contained herein are my own, etc..."

---

### **✂ Air Traffic in Leesburg VA**

*Peter G. Neumann <neumann@csl.sri.com>  
Tue, 7 Nov 1989 12:17:57 PST*

Friday evening's air traffic around Washington DC was awful. As most of you now know, both the primary computer system AND the backup were seriously degraded for at least two hours during the evening rush hour, stacking up and backing up air traffic extensively. (I was in DC that day. I'm at MIT today, Home tonight, hopefully.) The scuttlebutt seems to blame a buffer overflow, but I hope someone can contribute the real inside story.

---

### **✂ Equinox TV Documentary on "Fly By Wire"**

*Brian Randell <Brian.Randell@newcastle.ac.uk>  
Mon, 6 Nov 89 10:28:39 BST*

Last night the one-hour TV documentary in the Equinox series, entitled "Fly By Wire" was shown on Channel 4 in the UK. Since it was identified as "A Box Production for Channel 4, in association with WGBH/Boston, copyright 1989", I assume it will soon be shown in the States; I recommend looking out for it.

In my opinion it provided a reasonably complete and well-balanced (and also visually very attractive) account of the various incidents and opinions surrounding the A320, using a lot of well-chosen film clips, together with interviews with, or at least "sound-bites" from, about twenty different people.

>From Airbus Industrie there was Bernard Ziegler (VP Engineering), Roger Betaille, and Gordon Corps (Engineering Test Pilot) and, from Aerospatiale, Gilles Pichon (Chief Engineer A320) and Jacques Troy (Flight Control Manager). Four A320 pilots took part, including Michel Asseline, who alleged that his crash was due to the control-system over-riding his command to the plane to ascend. (The others were somewhat critical of the flight control system, but did not back up this allegation.)

The computing science community was represented by Mike Hennell, Bev Littlewood, John Knight, and John Cullyer. There were also representatives from Boeing, the FAA, CAA and DGAC, and Flight International.

The overall impression given was (i) that Airbus had been rather daring in introducing fly-by-wire, but had probably got away with it, and (ii) that their rivals would now follow suit, but that the next logical step, that of active control, was even more controversial and should not be rushed.

Brian Randell, Computing Laboratory, University of Newcastle upon Tyne, UK

---

### **✂ Lifethreatening risk! (related to Soviet PCs)**

*Julian Thomas <72355.20@CompuServe.COM>  
03 Nov 89 21:14:32 EST*

Seen on another news digest service (not in the original):

>From the Financial Times and the Daily Telegraph (UK) - articles about the Soviet Union studying a proposal to import lots of PC equipment for educational use. "The soaring demand for scarce PCs has swollen the Soviet crime rate, and PC owners have even been murdered for their machines."

Lock up your machines, gang, and compute only in the dark!  
Julian Thomas

---

### **✂ new computer risk: child abuse data base proposed**

*"W. K. (Bill) Gorman" <34AEJ7D@CMUVM.BITNET>  
Wed, 01 Nov 89 08:32:26 EST*

According to a news release heard a day or two ago, MI is now considering legislation permitting local communities to establish and maintain data bases of "suspected" child abusers, or those meeting another of the nebulous "profiles" used to identify all sorts of persons and ethnic groups in our society. Aside from permitting hearsay from neighbors, teachers, co-workers, associates and assorted third parties to be entered and disseminated about any particular individual or family, the framers of this legislation are also attempting to gain back-door access to medical records. One profile criteria disclosed for "identifying" child abusers is use of multiple doctors/hospitals by the same family. Physicians are threatened with legal sanctions for not reporting the simple fact that one or another patient HAS SEEN ANOTHER

PHYSICIAN without their knowledge/blessing. I don't think that implies any sort of involvement by Physicians or the AMA in this legislation.

Obviously, the privacy considerations and potential for misuse and/or malicious use, such as slanderous reports by neighbors against an unpopular neighborhood resident, inherent in this legislation are enormous.

---

### **✂ Dangers of mail aliases**

*Jonathan Leech <leech@cs.unc.edu>  
Wed, 1 Nov 89 18:43:52 EST*

Yesterday, I was surprised to find over a dozen messages from the internal technical mailing list of a company I worked for in 1982 in my inbox. As it turned out, the reason was that the mail alias a friend at this company used for me was duplicated in the systemwide alias file for a new employee. Fortuitously, nothing which was a sensitive matter (save for their code indenting style :-) happened to be discussed in the block of messages I received.

Jon Leech (leech@cs.unc.edu)

---

### **✂ Committee report on Bugs**

*<RMorris@DOCKMASTER.NCSC.MIL>  
Fri, 3 Nov 89 10:05 EST*

The congressional committee on Science, space, and technology issued this week a staff study entitled "Bugs in the Program: Problems in Federal Government Computer Software Development and Regulation". It is worth reading for those interested in risks. It is 33 pages long and I am not about to type any part of it in. It is available from the Sup of Documents, Congressional Sales Office, U.S.G.P.O, Wash., D.C. 20402. It does not have a reference number.

---

### **✂ Computer Viruses Attack China**

*Yoshio Oyanagi <oyanagi@is.tsukuba.ac.jp>  
Mon, 6 Nov 89 12:15:25+0900*

Ministry of Public Safety of People's Republic of China found this summer that one tenth of the computers in China had been contaminated by three types of computer virus: "Small Ball", "Marijuana" and "Shell", China Daily reported. The most serious damage was found in the National Statistical System, in which "Small Ball" spread in 21 provinces. In Wuhan University, viruses were found in \*ALL\* personal computers.

In China, three hundred thousand computers (including PC's) are in operation. Due to premature law system the reproduction of software is not

regulated, so that computer viruses can easily be propagated. Ministry of Public Safety now provides "vaccines" against them. Fortunately, those viruses did not give fatal damage to data.

Yoshio Oyanagi, University of Tsukuba, JAPAN

---

### ✂ First Virus Attack on Macs in Japan

Yoshio Oyanagi <oyanagi@is.tsukuba.ac.jp>

Tue, 7 Nov 89 17:07:09+0900

First Virus Attack on Macs in Japan

Six Macs in University of Tokyo, Japan, were found to have caught viruses, newspapers and radio reported. Since this September, Prof. K. Tamaki, Ocean Research Institute, University of Tokyo, has noticed malfunctions on the screen. In October, he applied vaccines "Interferon" and "Virus Clinic" to find his four Mac's were contaminated by computer viruses, "N Virus" type A and type B. He then found ten softwares were also infected by viruses. A Mac of J. Kasahara, Earthquake Research Institute, University of Tokyo, was also found to be contaminated by N Virus and Score Virus. Those are the first reports of real viruses in Japan.

Later it was reported that four Mac's in Geological Survey of Japan, in Tsukuba, were infected by N Virus Type A. This virus was sent from U. S. together with an editor.

Yoshio Oyanagi, University of Tsukuba

---

### ✂ NTT Challenges Hackers

<markw@gvl.unisys.com>

1 Nov 89 21:55:26 GMT

[A copy of the following article appeared on one of our bulletin boards here at work. I have no idea when or where it was originally published - MHW]

NTT: Calling All Hackers

Tokyo - Nippon Telegraph and Telephone Corp. has issued a provocative challenge: the Japanese communications giant will give 1 million yen (\$6803) to any computer hacker anywhere in the world who can break its FEAL-8 data communications security code by August 1991. Why the unusual move? The company wants to debunk a rumor circulating in Europe that its security code has been cracked. The FEAL-8 code, developed by NTT in 1986, is widely used in Japan and overseas to protect datacom systems and integrated circuit cards from illegal access.

---

### ✂ Even COBOL programmers need to know about range checking.

Bryce Nesbitt <bryce@cbmvax.commodore.com>

Fri, 3 Nov 89 17:40:53 EST

Last week I received this letter from my bank:

GREAT NEWS FOR THE HOLIDAYS!

Dear Bryce C. Nesbitt:

You are important to us. And, because of the excellent way you've handled your finances, we are pleased to increase the credit limit on your Meridian Open Line of Credit to \$0. Now you have more buying power when you need it most - in time for the holidays.

...

Thanks a lot. Before the promotion my credit limit was \$5,000.00. The rest of the letter talked about the free Mini-Vac that could be mine if I'd just borrow \$1,000 (funny, there was no mention of the over-limit penalty :-).

The bank had little to say about the event. I assume the calculation was based on a number of factors, including the "high credit" on the account. Since I have never drawn on this account, high credit would be zero.

---

## Unix Expo Power Failure

Jan I Wolitzky <wolit@mhuxd.att.com>

Fri, 3 Nov 89 15:17:10 EST

I was strolling through the Unix Expo show at the Javits Center in NY this morning, shortly after it opened for its third and final day, when all the power went out. My first reaction was that, boy, now we're gonna get to see whose systems really ARE uninterruptable. My second reaction was that there must be a VMS hack around somewhere. My third reaction, after it became clear that the lights weren't coming back on right away, was to move toward the daylight at the front of the convention center, with disturbing thoughts of panicked crowds, the San Francisco earthquake, and other paranoia in mind. As I approached the front of the hall, the big steel roll-up overhead doors started coming down. Quite a few people, apparently believing that their only exit was disappearing, rushed forward and ducked under the closing doors. It turned out that there were lots of other, conventional exit doors still available, but it still seemed to me a poor choice of failure mode: when the power fails (who knows, maybe because of a fire or other condition necessitating evacuation), close off the biggest and most obvious escape route. There was no panic this time, but after more than an hour, there was no power, either, so I gave up on the show. On the bus back, I was reading the issue of Unix Today that was being handed out at the show. A non-cover story described some of the problems experienced by the people who tried to set up an operating network (Ethernet?) at the show: apparently, some vendors were using unassigned net addresses, so that they could access other systems, but their competitors couldn't access theirs. And then there was the problem they had in actually laying the cable: normally a 4-hour job, it turned out that in NYC, it had to be performed by members of the Electrical Workers Union, who took 36 hours to

do it. I found the juxtaposition of the appearance of a story blasting the Electrical Workers Union and the power failure to be curious....

Oh yes, almost forgot, Unix is a registered trademark of AT&T.

Jan Wolitzky, AT&T Bell Labs, Murray Hill, NJ; 201 582-2998

att!mhuxd!wolit or jan.wolitzky@att.com

(Affiliation given for identification purposes only)



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 9: Issue 40

Friday 10 November 1989

## Contents

- ["Computer Error" in Durham N.C. election results](#)  
[J. Dean Brock](#)  
[Ronnie W. Smith](#)  
[John A. Board](#)
- [Glitch in Virginia election totals](#)  
[Paul Ammann](#)
- [Rome: Operator error causes publication of wrong election results](#)  
[Lorenzo Strigini](#)
- [Delayed Stock Exchange Opening](#)  
[Brian M. Clapper](#)
- [Electronic Warfare Systems not working--Congress](#)
- [Computer used to find scoflaws in Boston](#)  
[Peter Jones](#)
- [Computer errors and computer risks](#)  
[Randall Davis](#)
- [Equinox program on Airbus](#)  
[Lindsay F. Marshall](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✉ "Computer Error" in Durham N.C. election results

*J. Dean Brock <[brock@cs.unc.edu](mailto:brock@cs.unc.edu)>*

*Thu, 9 Nov 89 14:00:12 EST*

The headline on the November 9, 1989, Durham Morning Herald is  
Computer Twists Election Results  
According to the article a "computer error" caused eight precincts  
to be counted twice. The correction actually changed the result  
of one city council race twelve hours after it was assumed settled.

It's difficult to determine the nature of this computer error  
from the newspaper article. Another front-page article entitled:  
"Haywire Machine Counted Precinct Vote Totals Twice"  
quotes Jo Overman, the chairman of the County Board of elections, as saying:

One terminal used Tuesday apparently counted twice  
each precinct entered into it....  
What was called in was correct, the computer just added it twice....  
It was not added by an operator, it was a glitch in the program.

Ms. Overman, also added that the "errant terminal was an extra unit put on election duty as part of a last-minute effort to process returns faster."

Interestingly, the precinct-by-precinct breakdown given to the media was correct, even though they did not match the totals. The mistake was discovered in a later hand check of the results by the Board of Elections. Apparently, no one else bothered to check the totals.

The director of the county's Management Information Services department, which would be responsible for any programming errors, was instructed by the elections supervisor not to say anything about the election.

---

### ✂ "Computer Error" in Durham N.C. election results

*Ronnie W. Smith <rws@cs.duke.edu>  
Fri, 10 Nov 89 08:55:29 EST*

The only information I have to add is that the local TV media kept referring to it as a "computer error" without ever mentioning that the original source of the error was a person. The newspaper never explicitly made this link, but at least mentioned it was a programming error. Interestingly enough, the man who became the winner after he had been declared the loser did refer to it as a "human error". The number of votes that had been double added was slightly more than 6000.

Ronnie

---

### ✂ "Computer Error" in Durham N.C. election results

*John A. Board <jab@dukee.egr.duke.edu>  
Fri, 10 Nov 89 12:22:16 est*

[...] I find it most fascinating and troubling that it took over a day for anyone to notice that the correctly reported precinct votes duly tabulated in the paper the morning after the election did not add up to the numbers reported as totals at the bottom of the columns, and the errors were not small - the Mayor's race vote, for example, had been reported as 19,381 to 17,118 when in fact the real totals of the votes as listed were 16,136 to 13,356! To the credit of the elections board, the errors were apparently found during manual verification of the automatically reported "unofficial" results.

[With a "Duke" as Governor of both Massachusetts and California,  
I wonder if any Duke Univ. folks were governing this election? PGN]

## ✂ Glitch in Virginia election totals

Paul Ammann, George Mason University <pammann@gmuvax2.gmu.edu>

Thu, 9 Nov 89 14:25:22 -0500

In the Nov. 7 Virginia gubernatorial race, Doug Wilder (D) appears to have defeated Marshall Coleman (R) in a close race. Currently out of a total of 1.7 million votes, AP reports a difference of 5,533 votes and UPI reports a 7,755 vote gap. The Post article referenced below discusses the reasons for the discrepancies and the mechanism for official vote tallies. Buried within the article was the following gem: (Washington Post, Thursday, Nov 9, 1989, pp. A37, A40.)

Vote Counting Methods, Race Factor in Polls Leave Plenty of Room For Error  
Disparities Remain in Va. Governor's Race Tallies  
By Stephen C. Fehr, Washington Post Staff Writer

[discussion of discrepancies between AP and UPI vote tallies]

...

For an hour on Tuesday, [AP's director of planning Evans] Witt said, a computer glitch caused some of Wilder's votes in predominantly black precincts to be counted twice; the error was fixed and the vote total was adjusted.

...

AP's Witt said that "there's almost always a variation between the official and the unofficial count," but said he could not think of an instance in which the results of an election had been reversed because of a mistake by the wire services.

...

Comment:

There were many surprises and mistakes in the projections and reports of election results; the type of problem cited above is minor, but, left undiscovered, potentially quite serious. The decision to call for a recount, as well who bears the cost of a recount, depends upon the closeness of the election (according to the official tally, of course, which is due on the fourth Monday of November).

---

## ✂ Rome: Operator error causes publication of wrong election results

Lorenzo Strigini <STRIGINI@ICNUCEVM.CNUCE.CNR.IT>

Fri, 10 Nov 89 09:37:51 SET

On October 29-30, elections were held in Rome for a new city administration. Unofficial results published at first gave an important victory to the Christian Democrats, but at the end of the tallying this victory almost vanished. The publication of wrong results was attributed to a data-entry operator error. Since then, the political parties have been exchanging accusations of intentionally manipulating the data for political advantage (the supposed advantage would be a short-term boost in popularity for the Christian Democrats, or casting suspicions on the Christian Democrats, for the Communist). To set things in context: besides deciding who will manage the capital city of Italy,

these elections were regarded as an important indicator for national policy, and the major parties had put much effort in a combative, venomous campaign.

Now the details. (Disclaimer: this is my interpretation, checked with a few colleagues, of very imprecise press and radio reports. I'll look for more precise reports, and send in corrections if I can)

Voting and vote counting are by hand, with paper ballots. After the count started, and as partial results were transmitted from the individual "electoral sections", an EDP center of the City of Rome added them to obtain partial accrued results (without official value) and transmitted them to the press, radio and TV.

Very soon in this process, the published results showed a marked gain for the Christian Democrats. Later, it turned out that a few tens of thousands of extra votes had been erroneously given to them. The error became evident because the sum of the votes was greater than the number of voters. In an interview, the director of the EDP center stated that he had received from the computer program warnings about the discrepancy, but had ordered the publication of results to continue, assuming the problem was temporary and it would disappear later on.

Two days ago, the operator was found that allegedly caused the problem. He had to type in a screenful of data, send them to the computer and wait for it to clear the screen and prompt for new data (or to unlock the keyboard?). He found that pressing a certain combination of keys allowed him to clear the screen and restart input sooner, so speeding up his work. But by this trick he sent wrong data ("this affected the votes for 4 parties, and in particular the number of votes for the Christian Democrats -line 18 on the screen - was substituted with the number of the electoral section"). The program would complain about receiving inconsistent data, but give him an override option, which he used.

Now my comments. Funny: everybody is complaining about evil intentions (of which there's no proof), not about incompetence. From the news stories, some technical/organizational flaws are evident:

- the input routines checked for transmission overruns, or the application program ran consistency checks on each individual transaction (the entering of the results from a given number of ballots) but allowed the operator to override them (there was a log of the override requests, though: all inputs were logged to tape; but the log of part of the session was lost because tapes were scarce, and some were used twice).

- the director of the EDP center ignored the warnings (it is unclear whether these were from a global auditing of the data base or were the same error messages sent to the operator) about inconsistent data.

But, most important: in their greed for early results, both the press and the politicians trusted a non-trustworthy system. It appears that the only checks applied to this unofficial counting procedure were the consistency checks mentioned. If one were to bribe the operators to shift votes consistently from one party to another, this could go undetected until the official tally was available, several days later. The vulnerability so created is great: news reports of, say, an 80 % victory of the Communist Party would certainly hit the

Stock Exchange hard; the resulting allegations of fraud would cause a political earthquake (in the '50s, they might well cause a civil war). As things are, the effect on the public appears quite serious: according to an opinion poll, some 30 % of the voters interviewed said that, if the election were held again after the news of the mix-up was known, they would refuse to vote.

Lorenzo Strigini

Istituto di Elaborazione dell'Informazione, Pisa, Italy  
strigini@icnucevm.cnuce.cnr.it , strigini@icnucevm.bitnet  
IEI-CNR Via Santa Maria 46 I-56100 Pisa ITALY

[Regarding greed for early results, it was interesting to note that the advance polls in the New York City mayoral race were off by roughly 11%, and the exit polls were off by 10%. PGN]

---

### **✂ Delayed Stock Exchange Opening**

*Brian M. Clapper <bmc@SEI.CMU.EDU>  
Fri, 10 Nov 89 11:53:05 EST*

I received the following information from a friend of mine, William Power, who works as a reporter for the Wall Street Journal.

The New York Stock Exchange (NYSE) and the American Stock Exchange (AMEX) opened for trading approximately one hour late this morning (November 10) due to an inability to receive information from or transmit information to the Securities Industry Automation Corporation (SIAC), the jointly owned computer processing subsidiary of the two exchanges. SIAC suffered equipment damage due to a fire in its building at 55 Water Street in lower Manhattan. The fire apparently damaged equipment in a basement electrical vault, resulting in power outages to some areas of the building.

The initial fire alarm was posted at 8 am; the NYSE and the AMEX officially opened for trading at 10:30 am, one hour later than usual. The delayed opening resulted in a "domino effect," including the partial shutdown of the Chicago Mercantile Exchange.

Brian Clapper, Software Engineering Institute, Pittsburgh, PA 15213

---

### **✂ Electronic Warfare Systems not working--Congress**

*USENET NEWS <news@linus.mitre.org>  
8 Nov 89 14:19:36 GMT*

The Nov. 7 issue of the \*Washington Post\* carries a front page article on the failure of long-term EW development projects to deliver on their goals and to adequately counter 20-year old threat techniques.

The article describes a Congressional study, to be published soon, that looked at the B-2 bomber, and a service-wide EW system, now in its thirteenth year of development. Of particular interest is the criticism of the test methods,

described as not keeping up with the technology to be tested.

Although the article doesn't mention software specifically, the B2 software has been a significant issue.

My own experience in EW systems is that black projects seem to engender the attitude that since the project is not as visible, we can get away with less formal control and more ad hoc technical approaches.

Disclaimer: the truer it is, the stronger the denial.

---

### **✂ Computer used to find scoflaws in Boston**

*Peter Jones <MAINT@UQAM.bitnet>*

*Tue, 7 Nov 89 18:05:59 EST*

On Sun, 5 Nov 89 13:14:43 EST, "Barry C. Nelson" <bnelson@ccb.bbn.com>, in RISKS Volume 9 : Issue 39 said:

>

>When five out of six hits are human errors, imagine the complaints!

It goes to show the importance of considering the total effect of a system change, not just the project at hand. It was a serious design error to assume that licence numbers, even if they could be read accurately from a TV camera, could be used to positively identify wanted vehicles, if the database that indicates which numbers are "hot" is unreliable.

Peter Jones MAINT@UQAM (514)-987-3542

"Life's too short to try and fill up every minute of it" :-)

---

### **✂ Computer errors and computer risks (e.g., [RISKS-9.39](#))**

*Randall Davis <davis@ai.mit.edu>*

*Thu, 9 Nov 89 15:40:17 est*

Numerous stories have been reported on this list under the title "computer error" and "computer risk," that seem to me to have nothing essential to do with computers, and a great deal to do with very different issues.

Consider this story, for instance, from 9.39:

>Subject: new computer risk: child abuse data base proposed  
> According to a news release heard a day or two ago, MI is now considering  
>legislation permitting local communities to establish and maintain data bases  
>of "suspected" child abusers, or those meeting another of the nebulous  
>"profiles" used to identify all sorts of persons and ethnic groups in our  
>society. Aside from permitting hearsay from neighbors, teachers, co-workers,  
>associates and assorted third parties to be entered and disseminated,  
>the framers of this legislation are also attempting to gain back-door access  
>to medical records. One profile criteria disclosed for "identifying" child  
>abusers is use of multiple doctors/hospitals by the same family....

>

>Obviously, the privacy considerations and potential for misuse and/or  
>malicious use, such as slanderous reports by neighbors against an unpopular  
>neighborhood resident, inherent in this legislation are enormous.

If this is essentially a computer risk, there is an easy solution: get rid of the computer and we get rid of the risk. Modify the legislation to require that all database records must be kept manually on paper. If this story is really about computer risk, then all the problems noted above will disappear when the source of risk is removed. But do they?

Of course not. Because the problems are privacy, vague definitions, hearsay, backdoor entry, and interference in our lives. The technology used to accomplish those things is of some consequence (typically it changes the economics), but it is not of the essence. The real problems existed long before this particular technology and are largely independent of it.

It matters how we describe these things because descriptions implicitly set the agenda for discussion. To call it a "computer risk" is to set an agenda for discussing computers. This is particularly misguided when the questions that ought to be asked are: Should we collect such information at all? HOW we collect and store it will eventually matter, but the first and fundamental question is, shall we do it at all? What rights to privacy do we have? What modifications are we willing to make to those rights in pursuit of other, clearing conflicting goals in society?

In Mass., for example, (and perhaps elsewhere) doctors are required to report to a state agency evidence of child abuse (not just obvious cases, evidence). This is clearly a risky violation of the privacy of the doctor/patient relation, one that includes most of the problems noted above. The risks are reduced here because the information required is a professional opinion based on physical evidence. In this case it is a risk we accept, presumably because we believe the tradeoff is worth it. And \*that's\* what the discussion ought to be about: the risks and benefits of what we are doing, not what technology is used. The risks and benefits are often magnified by the technology, but the essential question is the risks/benefits of various sorts of privacy and the character of the information collected, not the technology that happens to be employed.

Of all groups, this list ought to get this right. Let me thereby enter a plea to use the term "computer risk" and "computer error" with considerable technical discretion. I suggest the simple test above: Ask, can the identical problem can arise in the absence of computers?

In some cases the answer is no (eg, instant, large-scale access to data from arbitrary distances), and these are essential, computer-related risks.

But if the same problem can arise, it is quite likely the technology is fundamentally irrelevant and that the risk involves something else. In that circumstance ask what the problem is normally called and use that name. The story above, for example, is about risks to privacy, the dangers of using inaccurate information from questionable sources, and requiring people to report one another's activities. Removing the computer from the picture does

not change those problems in any fundamental way. And the problems are serious enough that they ought to be debated on their own terms, without muddying the waters with technology.

---

### Equinox program on Airbus

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

Thu, 9 Nov 89 12:50:03 BST

I managed to get round to watching the program last night and found it very interesting. The program was very smooth except for one sound glitch - which occurred right in the middle of the word "reliability" when the narrator was discussing the multiple processor architecture...

Lindsay Marshall, Computing Laboratory, The University, Newcastle upon Tyne, UK  
NE1 7RU



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

**Volume 9: Issue 41**

**Saturday 11 November 1989**

## Contents

- [Stuffing the electronic ballot box \(again\)](#)  
[PGN](#)
- [BART and the Bartered-Computer Commuters](#)
- [Coral reef ruined by poor user interface design?](#)  
[Jim Helman](#)
- [Re: Computer errors and computer risks](#)  
[Jerome H Saltzer](#)
- [Computer used to find scoflaws in Boston](#)  
[David desJardins](#)
- [Reference on the early history of Ada -- killing reliably](#)  
[Eugene Miya](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **✉ Stuffing the electronic ballot box (again)**

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

Sat, 11 Nov 1989 13:30:42 PST

Charles Schwab & Co spent more than \$100,000 to conduct a nationwide poll on program(med) trading, with two widely advertised free 800 phone numbers set up to record the pro and con votes. Apparently someone at Wells Fargo (which has a high-profile program trading subsidiary) set up an autodialer to vote YES continuously, which was detected by their programmed monitoring. ( "First we have program trading. Now we have program dialing," quipped Senior Vice President Hugo Quackenbush. ) In 12 hours, there were 12,191 votes, 65.3% for, 34.7% against. [Source: San Francisco Chronicle, 11 Nov 1989, pp. B1-B2.]

[By the way, I observe that one call every twenty seconds for 12 hours would account for the entire difference between the pros and cons. One call every six seconds would have accounted for ALL of the pro calls. We might suspect that an autodialer could easily have skewed the results -- although perhaps others on both sides were also using the same strategy.]

---

## **✂ BART and the Bartered-Computer Commuters**

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

*Sat, 11 Nov 1989 13:46:02 PST*

The Bay Area Rapid Transit has for years been having troubles with its computer systems -- both old and new. The old one is supposed to handle 64 trains at once, but is barely able to handle 39. The new system -- almost ten years late when it went on-line three weeks ago -- was supposed to be able to handle 108 trains, but becomes seriously overloaded at 10. Consequently, all of the long-planned extensions are on hold. (The system supplier is Logica. The old system is still being used, at least as a backup when the new one is being tested.)

"An outside consultant that designed three control systems for the Paris Metro and was brought in by [BART General Manager Frank J.] Wilson has already determined that even if the new system were able to perform as promised, it is obsolete."

[A summary of "BART's New Computer Called `Complete Failure'", By Harre W. Demoro, San Francisco Chronicle, 11 Nov 1989.]

An earlier article indicated that the BART system has been sorely pressed in trying to accommodate the great increase in traffic due to the loss of the Bay Bridge in the earthquake, and many train cars are out of service.

---

## **✂ Coral reef ruined by poor user interface design?**

*Jim Helman <helman@isl.Stanford.EDU>*

*Fri, 10 Nov 89 19:09:37 -0800*

The captain of a ship which ran aground on an environmentally sensitive live coral reef off the US coast attributed the accident to a confused officer and a bad user interface. Apparently, an officer incorrectly changed course because the steering mechanism on the ship operated in the opposite fashion from most such controls.

Whether or not the control was computerized, this demonstrates quite dramatically the potential dangers of inconsistent user interfaces. I suppose the company which built the control could be held liable for the poor design.

There may be parallels with GUI issues yet to come. What if a company has to use an inconsistent interface because of patent restrictions? Could the company still be liable for the errors of a confused user?

Excerpts from the UPI article follow:

``I think he made an error. I think he was confused," Capt. Zdravko Beran told Coast Guard investigators on the first day of testimony before a board of inquiry. ``He told me that (navigational) light was dead ahead and then he wanted to turn a few degrees to the port (left)."

Instead, the officer, Zvonko Baric, turned the ship to the right, or starboard, causing it to run aground on sensitive coral in the Fort Jefferson National Monument, Beran said.

The steering mechanism must be turned in the opposite direction of the intended course -- the reverse of how most such devices operate, Beran said.

Asked how future such accidents could be avoided, Beran said the federal officials could require ships to go around rather than through the national monument.

Jim Helman, Department of Applied Physics, Stanford Univ., Stanford, CA 94309

---

**✉ Re: Computer errors and computer risks ([RISKS-9.40](#))**

*Jerome H Saltzer <[saltzer@src.dec.com](mailto:saltzer@src.dec.com)>  
10 Nov 1989 1613-PST (Friday)*

In [RISKS DIGEST 9.40](#), Randy Davis says,

> Numerous stories have been reported on this list under the title  
> "computer error" and "computer risk," that seem to me to have nothing  
> essential to do with computers, and a great deal to do with very  
> different issues.  
> . . . I suggest the simple test above: Ask, can the identical  
> problem can arise in the absence of computers?

I claim that it is not that simple. In a traditional library, it was possible to invade your privacy by making a list of all the books you have every checked out. All an investigator had to do was open every book in the library and look to see if you had signed the card inside. The information was publicly available, but actually it was benignly protected by an enormous collection cost, so noone every worried about it.

These days, if the library has a computerized circulation system, and it is not designed with proper regard for privacy, it may be possible to get this information in a few seconds with a single request. Most computerized circulation system protect this information and many installations systematically delete it to avoid any possibility of such investigations. Yet, when the first circulation systems were designed, some people said that the circulation information has "always been public" as an argument against protecting the information in the computerized system.

The Registrar of Motor Vehicles in Massachusetts has long used the "it has always been public" argument on car registration information as an excuse for selling tapes to mass mailers. But as I recall, I didn't receive that class of junk mail back in the days when you had to personally visit the Registry and copy the information out of their ledgers.

The point is that the speed and efficiency with which data can be processed by

computer can convert a negligible risk into one worth discussing. Had the RISKS forum been around then, I think the library debate would have been quite an appropriate topic. Ditto the Mass. Registry.

Finally, the availability of the computer to discover connections may tempt people to create data bases that they wouldn't otherwise consider feasible. When I saw the report in RISKS on the proposed child-abuse data base I assumed that this was an example of a data base that probably wouldn't have been proposed had computers not been available to implement it--especially the part about identifying people who use multiple doctors.

Thus I am prepared to tolerate a certain amount of fuzziness in identifying the edge of the computer-RISKS arena by our beleaguered moderator.

Jerry Saltzer

---

### **Computer used to find scoflaws in Boston**

*David desJardins <desj%idacrd@Princeton.EDU>*

*Fri, 10 Nov 89 21:01:38 EST*

<>When five out of six hits are human errors, imagine the complaints!

>

> It goes to show the importance of considering the total effect of a system

> change, not just the project at hand. It was a serious design error [...]

I am very surprised at how much complaining there has been about this error rate. I think finding one stolen car in every six stopped is a phenomenally *\*high\** success rate. It doesn't seem a major problem to me to inconvenience five people for a relatively short period of time in order to apprehend one serious criminal. I would think almost any other form of police work would involve a much higher level of inconvenience to the public for the same level of success.

For comparison of order of magnitude, look at neutron-activation bomb detectors, to be installed in airports. They are said to have something like a 3% false positive rate (and that is in controlled tests, so the real rate will most likely be higher). I don't have a number at hand for the actual rate of bombs in checked luggage, but let's say that it is 1 in 30 million (I'm sure it is less). That corresponds to 1 million false positives for every true positive. *\*That\** is a high rate of error. And our society has chosen to spend nearly a billion dollars on that system.

-- David desJardins, IDA/CRD

---

### **Reference on the early history of Ada -- killing reliably**

*Eugene Miya <eugene@eos.arc.nasa.gov>*

*Fri, 10 Nov 89 23:21:42 PST*

I finally had a reason to dig thru the same box which had the following reference in the history of Ada. The quote comes from Pascal News #13, December 1978, then published by the Pascal User Group. This is a bound journal (although basically Xerox(tm) copied sheets); it was unrefereed. By

way on context, it should be recalled that the initial proposals for the new DOD language (then referred as DOD-1, various "colors," and the progression: Strawman, Woodenman, Tinman, Ironman, and then Steelman) had 17 proposals based on Pascal (the last was based on PL/1, you can guess who proposed that 8). So, the Pascal community was thrust into the limelight. (It was still a somewhat obscure language at the time.) The quote is authored by Andy Mickel, U MN, then the editor:

Latest News About DOD-1 (ADA or DOD0) --Andy Mickel

As we've told you in previous issues of Pascal News, the U.S. Department of Defense (DOD) has endeavored to procure a common programming language based on Pascal for all "embedded" computer applications -- computer systems attached to weaponry. Reliable software should kill people reliably! .....  
[above description removed] ...colors: BLUE-Softech, GREEN-Honeywell Bull; RED-Intermetrics; and YELLOW-SRI International.

The article goes on for two more paragraphs, but Andy's comment about killing was not taken lightly. Pages 9-10. So much for the history of programming languages.

--eugene miya, NASA Ames Res. Ctr.  
formerly joint ANSI X3J9/IEEE P770 Pascal Language Standards Committee



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 9: Issue 42

Monday 13 November 1989

## Contents

- [Equinox TV programme on A320](#)  
[Bev Littlewood](#)  
[Chris Dalton](#)
- [European Safety is not always BETTER](#)  
[Bruce C. Brown](#)
- [Artificial lightning](#)  
[PGN](#)
- [Another intrusive database with associated privacy problems](#)  
[Bill Gorman](#)
- [Re: "Computer Error" in Durham N.C. election results](#)  
[Gregory G. Woodbury](#)
- [Re: Computer errors and computer risks](#)  
[Willis H. Ware](#)  
[D. King](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✉ Equinox TV programme on A320

*B.Littlewood <sd396@CITY.AC.UK>*

*13 Nov 1989 17:42:48-GMT*

Brian Randell, in [RISKS-9.39](#), gave a brief description of this programme, which he thought was quite well done. I have a few more reservations than Brian, but this may be because most of the film of me ended up on the cutting-room floor!

There were some interesting moments, though, not least in some of the assertions still being made by Airbus and its constituent companies. Throughout there was a curious belief in the power of the 'systems approach'. Perhaps the strongest statements came from Gilles Pichon (Chief Engineer, A320, Aerospatiale), who said:

"Safety is ensured by the system approach: the computers, the sensors, the whole environment, the power sources and the computer software. All this has

to be analysed very closely for safety. And the method of analysis, which is called safety analysis, has been around for over 20 years. It was used for Concorde and it's still valid today."

Pretty unexceptionable, you may think, but this statement is quickly followed in the film by a more detailed examination of the fault-tolerance of the fly-by-wire system:

Jacques Troyes (Flight Control Manager, Aerospatiale): "We work with three pieces of information completely independent of each other. And we can only guarantee to protect the aircraft with certainty when we are sure of having at least two pieces of information."

I assume this is a reference to the A320 software fault tolerance, but if so it is a bit confusing. The voice-over questions whether developing all versions from the same specification might introduce common faults. Then cut to

John Knight (University of Virginia): "It appears to be possible to build diverse programs where the programs will allow you to recover from certain kinds of difficulties that the software may get into. The real issue is we have no way of predicting ahead of time how successful that kind of technology is going to be."

Voice-over then says Airbus have stated the system is designed to fail only once  $10^{*-9}$  hours [lovely slip that -- they mean  $10^{*9}$ !]. Then cut to me

Bev Littlewood (City University): That means this system should fail every billion flight hours. A billion flight hours is about 100,000 years. There is no-one in this business believes you can design systems to that reliability."

Pichon: "Having done all our safety analysis we are confident that we achieved the  $10^{*-9}$ . And for those who have some doubts we can also say that even with no fly-by-wire the aircraft can fly safely because we have the mechanical back-up at the end."

Voice-over explains that mechanical back-up is really only meant to keep the aircraft flying until computer system is got working again.

Littlewood: "Airbus could have had a fully functioning mechanical back-up on that aircraft, so that in the event of total loss of the computer system it was still flyable. Now what they've got is a vestigial mechanical back-up. Really all that you can control if you totally lose the computer system is the rudder and tail trim."

Gordon Corps (Engineering Test Pilot, Airbus Industrie): "I had one Northwest Airlines pilot land the airplane totally satisfactorily using just the back-up system."

Later in the film, there is an interview with Michel Asseline, who was pilot in charge of the A320 which crashed on the Mulhouse flight.

Asseline: "When I pull the stick to up position, the flight controls, the elevator controls, go to down position . . . why? That would be the good

question."

Whereupon a man from the DGAC (the French certification agency) is asked whether he had seen any evidence to support this claim. He said he had not. Then cut to

Bernard Ziegler (Vice-President, Engineering, Airbus Industrie): "By no means, never, the computer want to land the aircraft, never. I would even say, believe it or not, that we have put in our computer law to resist to land. The pilot land the aircraft, and nobody else."

The voice-over then comments that, 15 months later, the official French report into the crash has not been published, but it will almost certainly clear the computer.

Later there are reports of other problems pilots have met, including the following exchange

Gino Scattolini (A320 pilot): "As we were coming in to land with the engines at idling speed, the two engines accelerated up to climbing speed, and as the automatic systems were not working we might have left the plane's flight path if the crew had not intervened. But safety was never at risk."

Corps: "There have been fine tuning changes done in some aspects of the software and I guess they will go on for some time, as we say just to cure some of the teething problems that we have seen. But they haven't affected anything of significance associated with flight safety at all."

The film ends by looking to the future, and in particular the possibility of unstable commercial aircraft.

Ziegler: "It's clear that we say active control, which is a natural derivative of the fly-by-wire, we will be able to reduce the weight of the structure, to reduce the surface of the control. That is also the next step and we are working also in this direction."

Littlewood: "Now making an airliner unstable would bring enormous economic benefits because it would cut down drag and the aircraft would be much more fuel efficient. But an unstable aircraft has to be controlled by computer all the time; there is no possibility of a mechanical control by the pilot. So that next step is one I think we ought to be worrying about."

Brian Perry (UK Civil Aviation Authority): "There's nothing we know which would say we shouldn't consider such an approach. We believe that if you take the system approach which looks at the hazards following system failure or system non-availability, and can satisfy yourself that the safety criteria are met, then the aircraft is potentially certificatable."

Certainly I agree with Brian that the film is worth seeing (I think it is to be shown in the US -- probably on Public Broadcasting). It would have been good to have more debate and less lovely pictures of the A320 doing fancy things. But a couple of things did come out.

First, it seems that senior engineers (Pichon, above) are still trying to convince us that they have achieved the mythical  $10^{-9}$ . Are they fools or knaves?

Second, there seems to be confusion about exactly what can be expected of the back-up system. Do Airbus want us to believe that airline pilots will be able to land on this, or that they will never need to do so? (or both?)

Third, there have been software problems. (I'm intrigued by the notion of 'fine tuning': is this similar to 'it's not a bug it's a feature'?)

Fourth, this was the first formal statement I had heard that Airbus were working on active control. It seems to me that the certification agencies have to take a more active role here than is represented by Perry's statement.

BEV LITTLEWOOD, Centre for Software Reliability, City University,  
London EC1V 0HB

---

### **✂ Mistake in Equinox "Fly-by-wire" programme**

*Chris Dalton <crd@hplb.hpl.hp.com>*

*Mon, 13 Nov 89 14:53:55 gmt*

The Equinox programme mentioned by Brian Randell and Lindsay Marshall in Risks 9.39 and 9.40 has a glaring mistake in the script... I hope.

The announcer quite clearly explains at one point that the system was designed to fail every "ten to the minus nine hours". Moments later, an engineer says they achieved the " $10^{-9}$  error rate". (I'd recorded the programme, so I was able to check what was said.)

A case of losing something in the translation?

Chris Dalton Hewlett-Packard Labs, Bristol BS12 6UF, UK +44 272 799910  
crd@hplb.hpl.hp.com crd@hplb.lb.hp.co.uk ..!mcvax!ukc!hplb!crd

---

### **✂ European Safety is not always BETTER**

*Bruce C. Brown <bcbrown%fnal.dnet@fngate>*

*Sun, 12 Nov 89 23:17:10 CST*

Recent discussions in RISKS have suggested that safety standards in Europe are superior to those we enjoy here, and indeed, some recent statistics suggest that that may be true in some important senses. However, we should beware in adopting the stance that they have the answers and we have nothing to give.

In particular, I was in Hamburg, Germany for a six month assignment in 1987 and was AMAZED to discover that the American safety requirement that all door open OUT and that buildings have doors which are locked such that noone can be locked in were unknown there. If I forgot my keys and worked late, I could be locked in at three separate levels: my own office, the office corridor, and the

building external doors. MOST rooms had telephones, but...

Like everything else, we need to be careful about adopting anything wholesale, without review.

Bruce C. Brown, Magnet Test Facility,  
Fermi National Accel Lab, Batavia, IL 60510

---

## ⚡ Artificial lightning

"Peter G. Neumann" <neumann@csl.sri.com>  
Mon, 13 Nov 1989 16:19:48 PST

Lightning may be natural, or may actually be stimulated artificially by man-made conditions in situations in which lightning might otherwise not occur. The latter occurred in the second and third of the following cases:

... three spectacular lightning accidents involving aircraft or spacecraft:  
(i) In 1963, a Boeing 707 flying at 5000 feet near Elkton, Maryland, was struck and destroyed by lightning, killing all occupants (3). Lightning apparently burned through one of the metal wings, or in some other manner entered the fuel tank inside that wing, and caused the fuel vapor there to explode. (ii) In 1969, Apollo 12 artificially initiated (or "triggered") two lightning flashes, one to ground and one intracloud (IC) discharge, when it was launched through a weak cold front that was not producing natural lightning (4). Although this rocket-initiated lightning caused major system upsets and minor permanent damage, the vehicle and its crew survived and were able to complete their mission successfully. (iii) In 1987, an unmanned Atlas-Centaur vehicle (AC/67) was launched into weather conditions that were similar to those present at the launch of Apollo 12 and triggered a lightning discharge to ground (5). This discharge upset the computer memory in the vehicle guidance system and produced an unplanned yaw rotation, and the associated stresses caused the vehicle to break apart.

This paragraph is excerpted from an article in the 27 October 1989 issue of *Science*, Natural and Artificially Initiated Lightning, by Martin A. Uman and E. Philip Krider, pp. 457-464. References 3-5 are given in the article.

The Atlas-Centaur case was previously reported in [RISKS-4.70](#) (1 April 1987, no joke) and [RISKS-4.96](#) (6 June 1987). The Apollo 12 case has not -- to the best of my knowledge been noted here previously. More generally, the detailed discussion of artificially triggered lightning in the *Science* article should be particularly interesting to RISKS readers.

---

## ⚡ Another intrusive database with associated privacy problems

"W. K. (Bill) Gorman" <34AEJ7D@CMUVM.BITNET>  
Mon, 13 Nov 89 14:00:50 EST

MEXICO AND USA SIGN TREATY TO ATTACK TAX EVASIONS

The Mexican Secretary of Treasury, Pedro Aspe Armella, and Nicholas Brady, North American Secretary of Treasury signed a treaty to detect and combat tax evasions on both countries. By means of this treaty both nations will have access to information concerning the income of Mexicans living in the States and of North Americans living in Mexico. This deal also establishes the possibility to exchange information on people who evade taxes. This data will be exchanged only if the laws and rights of the citizens are respected in each country. With this information, the fiscal authorities expect to detect possible tax evasions by incomes obtained in another country and that are frequently not reported to the Government.

[... another privacy "loophole" via a shared data base. The comment about protecting privacy by "observing all laws of both countries" is absurd. Once the data is in the hands of any third party, individual, corporate or national, controls imposed from without are nothing more than "gentlemen's agreements" observed out of courtesy and/or convenience. Bill]

[Bill did not indicate where this appeared. I edited it lightly to fix a few typos (e.g., Treasure), but left "North American Secretary". PGN]

---

### ✂ Re: "Computer Error" in Durham N.C. election results

Gregory G. Woodbury <ggw@wolves.uucp>

Tue, 14 Nov 89 02:51:39 GMT

- > [With a "Duke" as Governor of both Massachusetts and California,
- > I wonder if any Duke Univ. folks were governing this election? PGN]

Well, I work at Duke University, and I was also working as an assistant to the precinct registrar for my home precinct -- that might count a "governing" this election ;-)

It was an enlightening experience doing an election. The machines used around here are purely mechanical. The only electricity used is for a fluorescent light over the front panel. After the election, a hand crank is used to force the counter wheels against an NCR paper (or rather vice versa) and the numbers are transcribed by hand to the official ballot reports.

In my precinct, we had two calculators (electronic) to assist in the tally, and I still caught an error by doing a simple parity check on the numbers as they were called out.

As for the "Computer Error" down at the Board of Elections... What goes on there is simply a convenience for the press and candidates. The BoE staff has a few PC's and spreadsheets set up to do simple calculations and the person who got to put it together this year simply messed up one of the cross-tabulations. There is not, as far as I know, a specific program that the BoE uses, just a PC set up in the County Commission meeting room used for simple arithmetic. Prior to last year they used simple hand calculators and never had a problem.

The "Official Election" comes about one week after the voting when the registrars from each precinct sit down "en banc" and canvass the actual numbers from the machines in their precincts and double check each other via whatever method is most convenient. Some of the registrars actually do the arithmetic in their heads and have the result written on their

scratch pads before the various calculator people can announce what they get. All in all, its still dependent on mechanisims and mental skill.

Gregory G. Woodbury, Sysop/owner Wolves Den UNIX BBS, Durham NC

---

**✂ Re: Computer errors and computer risks (Saltzer, [RISKS-9.41](#))**

"Willis H. Ware" <willis@rand.org>

Mon, 13 Nov 89 16:05:42 PST

<> ..... In a traditional library, it was  
<> possible to invade your privacy by making a list of all the books you  
<> have every checked out. All an investigator had to do was open every  
<> book in the library and look to see if you had signed the card  
<> inside. The information was publicly available, but actually it was  
<> benignly protected by an enormous collection cost, so noone every  
<> worried about it.

In privacy discussions, one frequently hears the point about convenience of collection, magnitude of what can be obtained for little effort, etc., but the concept of "benign protection by the status quo" is a very adroit way of capturing the point and of relating it lay folks.

His point also brings to mind one made very forcefully by Richard Hamming (currently on the faculty of the USN Postgraduate School at Monterey, CA) many years ago. In paraphrase, he said: "when something changes by an order of magnitude, there are fundamental new effects."

Certainly from the benign library of the past to the computerized one of now, the effort to assemble one's reading list has changed by been many orders of magnitude.

Hamming's Law is really what's behind so many of the computer-induced effects, and it's also the underlying issue in having such effects understood among the laity. It's certainly a big part of the problem with getting legislators to pay attention; they think everything is fine just because it has been fine in the past.

Willis Ware

[Hamming is also well known for not standing on Isaac Newton's feet. PGN]

---

**✂ Re: Computer errors and computer risks (Saltzer, [RISKS-9.41](#))**

<king@kestrel.edu>

Mon, 13 Nov 89 09:54:08 PST

<> In <a href="/Risks/9.40.html">RISKS DIGEST 9.40</a>, Randy Davis says,  
<> > . . . I suggest the simple test above: Ask, can the identical  
<> > problem can arise in the absence of computers?  
<> > I claim that it is not that simple...

I think i must respectfully disagree.

Consider the two examples given ... Yes, i will concede that the cost of collecting library patron information precludes its use to send "appropriate" junkmail. The cost of collecting DMV information precluded its use for junkmail as well. But these are trivial invasions of privacy, and not the ones i'm most worried about.

Consider the possibility of a new McCarthy Era. During the old McCarthy Era, readers of certain books in the library WERE found and used for purposes which i would assume many would just as soon forget. The fact that this information was available in dilute form protected nobody. Recall that both the imaginary but believable society of 1984, and the real tyranny of Nazi Germany, were quite plausible/possible with only "human computers".

Consider the case of the skiptracer. The cost of a DMV trip would be a negligible portion of his cost of doing business; no doubt he would have several cases he could service with a single trip.

So, in part, i support the original thesis that for serious breaches of privacy [as opposed to trivial annoyances] lack of a computer is no protection against data collection. In part, i offer a possibility for a NEW protection.

It is practical for the head librarian of even the largest city to personally walk the half-dozen disk packs containing circulation information to the library's degausser, together with the appropriate tapes, and defend the privacy of the more-than-two-month-old circulation information reasonably absolutely. It is possible for the populace to order the DMV to implement access poicies. In short, the compactness of the information implies that the privacy afforded patrons of a particular service will not be the accidental result of the way things happen to be, but the result of an explicit decision.

-dk



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

**Volume 9: Issue 43**

**Wednesday 15 November 1989**

## Contents

- [L.A. Times Computer Foulup](#)  
[Jerry Hollombe](#)
- [Altered bits in Risks 9.39](#)  
[John M. Sullivan and Henk Langeveld](#)
- [Re: Apollo 12 \(Artificial lightning\)](#)  
[Henry Spencer](#)
- [Re: Equinox TV programme on A320](#)  
[Alan Marcum](#)
- [Failure of Systems After Earthquake](#)  
[Jon von Zelowitz](#)
- [Article about "Paperless Office"](#)  
[Alan Marcum](#)
- [Are you sure you declared ALL your dividends?](#)  
[Peter Jones](#)
- [Re: Another intrusive database ...](#)  
[Jim Horning](#)
- [Re: Computer errors and computer risks](#)  
[David Smith](#)  
[John Locke](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **L.A. Times Computer Foulup**

*The Polymath* <[hollombe@ttidca.TTI.COM](mailto:hollombe@ttidca.TTI.COM)>  
14 Nov 89 02:21:45 GMT

Here's a first-hand experience, for a change:

Some months ago my SO subscribed to the L.A. Times newspaper. She made it very clear she wanted the Sunday edition only. A week later papers began arriving -- every day. We called the Times and complained. The person who answered looked us up in their data base. Sure enough, we're listed there as Sunday edition only. She said not to worry about it, we would only be billed for the Sunday papers.

Time goes on. Daily papers continue to arrive. We complain again. (We don't want daily papers. Not even for free). Same story. The computer has us listed as Sunday only, so we shouldn't worry about it.

More time. More daily papers. Recycling them is becoming a major nuisance. On our third, most recent call the Times operator asked "What is it you want?" We answered "Sunday delivery only." "Well, the computer says that's what you're getting." End of conversation.

We're still getting daily papers. )-:

The Polymath (aka: Jerry Hollombe), Citicorp(+)TTI, 3100 Ocean Park Blvd.,  
Santa Monica, CA 90405 {csun|philabs|psivax}!ttidca!hollombe

---

### **✂ Altered bits in [Risks 9.39](#)**

<sullivan@math.Princeton.EDU>

Wed, 15 Nov 89 19:36:25 -0500

I get my news from phoenix.princeton.edu, and on that machine, [RISKS-9.39](#) arrived AFTER [9.40](#) and [9.41](#). Furthermore, many characters had been altered, having their 2<sup>nd</sup> bit set. The most common changes were ' ' -> '\$' (happened 30 times) and 'h -> l' (there were many instances of the word "tle"). I also noticed y->}, s->w, i->m, p->t, b->f, r->v. Note that in all of these cases, the letter substituted has ascii value exactly 4 greater than the original (one extra bit set).

John M. Sullivan Princeton Univ. Math Dept. sullivan@math.princeton.edu

[Similar behavior was reported by several other recipients, including henk@cs.eur.nl (Henk Langeveld) in Rotterdam, whose return path to me was "eurai1!eurtrx!hp4nl!mcsun!uunet!seismo!ukma!tut.cis.ohio-state.edu!gem.mps.ohio-state.edu!usc!ucsd!ames!lll-lcc!unisoft!mtxinu!ucbvax!CSL.SRI.COM!risks". His copy had an interesting FROM: field -- "From: rmsks@CSL.SRI.COM (RISKS Forum)".

We have reported previously on compression screwups making systematic substitutions in software. This one looks like a transient hardware bit error in the 4's bit, somewhere along the line. I hope someone can track down its origin. This is the kind of thing that simply shouldn't happen anymore. Reliable protocols? Bah, humbug. PGN]

---

### **✂ Re: Apollo 12 (Artificial lightning, [RISKS-9.42](#))**

<henry@ut zoo.UUCP>

Wed, 15 Nov 89 13:35:23 EST

An interesting sidelight is *\*why\** Apollo 12 survived the lightning strikes. The Apollo spacecraft's electronics got scrambled quite thoroughly, but the independent computers running the Saturn V booster were unaffected. They were

in a much less exposed position, on top of the booster proper, underneath the Apollo spacecraft assembly. (They may also perhaps have been better protected against electrical upsets, although I don't know that for sure.)

Early in the Saturn program, there had been some discussion of the idea of saving weight by having the spacecraft computers run the booster as well; Wernher von Braun vetoed the idea and insisted on the booster having its own control system. This was probably more because of potential problems with changing payloads -- the Saturn V was meant to be NASA's heavy booster well into the 1980s, launching much more than just Apollo -- but I seem to recall that better protection for the electronics was mentioned as well.

Henry Spencer at U of Toronto Zoology

---

### **✂ Re: Equinox TV programme on A320 (from 9.42)**

<Alan\_Marcum@NeXT.COM>

Tue, 14 Nov 89 09:36:34 PST

Truth stranger than fiction? Several months ago, I stumbled on a novel, *\_Passengers\_*, copyright 1983, by Thoms G. Foxworth & Michael J. Laurence. It tells the story of a brand new airliner with active fly-by-wire controls and inherent aerodynamic instability. The book does have some technical flaws. However, it happens to cover not just the active fly-by-wire issue, but also whistle-blowing and different international safety standards and evaluations.

Again, not one's most technically accurate source, but an enjoyable read nonetheless, especially in light of many of the discussions on RISKS.

Alan M. Marcum, NeXT Technical Support (415)780-3753

---

### **✂ Failure of Systems After Earthquake**

Jon von Zelowitz <vonzelow@adobe.com>

Mon, 13 Nov 89 23:12:05 PST

An article in the San Francisco Bay Guardian of November 9, 1989 entitled "We Almost Lost San Francisco", and an accompanying sidebar "Water, Water Everywhere..." investigate some of the failures and near-failures of major systems during the October 17th earthquake. Most failures were made up for by individuals' dedication and heroism.

According to the article, years of budget cuts and neglect had left the City unprepared for such a disaster. Here is a summary of some of the points in the article.

The telephone system held up pretty well, but the 911 system (not intended for a disaster) was overloaded. There are only a few 911 trunk lines from each exchange, and only 15 lines go into the 911 operators.

With 911 flooded, the primary way for citizens to contact the fire department was the Street Telegraph System, which was first built in 1875, and reconstructed after the 1906 earthquake. The Fire Department had defended the system from former Mayor Feinstein's budget axe. The telegraph system is triggered by pulling alarm boxes along city streets, sending a coded signal to a teletype at the Central Fire Alarm Station. Because the alarm boxes contain spring-driven works, and the telegraph lines are battery-powered, the boxes worked fine after the quake.

Unfortunately, the success story of the street boxes ends there. The telegraph messages are decoded by a 16-year-old DEC computer. It has a history of crashing under heavy load, and went down almost immediately after the quake. Dispatchers ended up using an antiquated 1940's-era card system called "the tubs" to identify the locations of alarms and assign units. A department chaplain used a pegboard to keep track of assignments.

Fire Commissioner Sharon Bretz told the Bay Guardian that no computer could have handled the flood of calls into the Central Fire Alarm System.

The City's police, fire, and ambulance radio works through a repeater on Twin Peaks, the highest point in town. When electrical power failed, emergency generators kicked in. They are so old that mechanics can no longer obtain spare parts for them. Both had trouble with their water pumps. The first one overheated and failed; luckily, a dedicated engineer kept the second unit (an identical machine with identical failure mode) running.

A large fire broke out in the Marina district. Water was eventually supplied by the Phoenix, an aging fireboat. There is a special high-pressure water system specifically designed to supply water for firefighters after an earthquake, but no one ordered it turned on. Even if the order had been given, some of the pump stations are unmanned and automated, and have no generators; the electrically-operated valves would not have worked. And some of the dozen workers who know how to operate the system live out of town.

[I was lucky -- no damage to my home, and no nearby fires. I headed for the neighborhood bar for some warm beer, and returned home when power came back on (around midnight). -jvz]

...sun!adobe!vonzelow vonzelow@adobe.com Jon von Zelowitz

---

## **✂ Article about "Paperless Office"**

<Alan\_Marcum@NeXT.COM>

Tue, 14 Nov 89 14:06:00 PST

Here's an article someone at work sent to me. I find the perspective of the author, um, interesting, and offer it to the group for their perusal, amusement, and comment.

No more John Hancock

Businesses start to sign off on paperless deals

By Tom Steinert-Threlkeld Dallas Morning News

DALLAS. Until now, the operative phrase for sealing a contract has been, "Put your 'John Hancock' on the line." Soon, that may change. The operative phrase could well become, "Send your personal identification code over the line."

Such is going to be the impact of the paperless contract. Unlike much of the rest of the "paperless office," electronic purchase orders, invoices and payments are taking off.

The process is called electronic data interchange. EDI involves a variety of protocols and standards for paperless communications allowing companies to buy and sell goods and services to each other simply by sitting at a screen on a desk. EDI is growing rapidly. Dallas attorney Benjamin Wright, author of a new book called "EDI and American Law: A Practical Guide," estimates that as many as 7,000 firms and agencies worldwide now use electronic means for conducting basic business transactions.

Market Intelligence Research Co. estimates that only \$11.3 million of business was conducted through such means in 1985. That will have grown to \$144.7 million of EDI business this year, the Mountain View research firm estimates. By 1993, use will grow to \$1.1 billion, the company says. Two years later? \$1.8 billion. EDI is here to stay.

But the John Hancock problem remains. How do you prove that an electronic document is for real? As computer malfeasance has proved, electronic information can come from anywhere and go to anywhere. No fingerprints get left. No signatures are affixed. Heck, for that matter, make the wrong move and the whole blasted thing gets erased in a blink. And there are no carbons. It's not quite as bad as all that. As Wright notes, electronic documents frequently can be more secure than paper documents. Electronic systems provide a multitude of options for automatically securing and authenticating documents or data: passwords, security codes, encryption, and the like.

In addition, the information is less susceptible to damage. With electronic transactions, basic information on a transaction need only be typed one time. Let's say your company sends a quote to a customer. The customer gets the quote. Electronically, the customer can reuse the data when it sends back an acknowledgment of receiving the quote. From then on, through purchase order, invoice, statement and payment, the data remains the same. No errors get added at each step, from separate data entry operators.

Even if there is an error, it gets identified and fixed more rapidly, by electronic means.

The systems can even automatically generate an electronic trail to follow complex transactions and ongoing business. Acknowledgments, tracking numbers, audit logs, network transmission reports there's a wealth of information that can be logged by electrons, instead of by hand.

This is no small matter when you're trying to prove a transaction took place. You can't haul electrons into court. You still will have to take paper, even if it is a printout of the transaction that actually was stored magnetically on tape.

And you won't be able to show that you signed off on the deal. Paperless transactions also mean signatureless transactions. The basic means of sealing deals for centuries is giving way in a matter of years.

Alan M. Marcum, NeXT Technical Support (415)780-3753

---

### **✂ Are you sure you declared ALL your dividends?**

*Peter Jones <MAINT@UQAM.bitnet>*

*Tue, 14 Nov 89 18:43:49 EST*

On CBC radio this morning, during the Daybreak program, there was an interview with a tax expert by the name of Benoit Lasalle. Mr. Lasalle was warning taxpayers that some people were getting letters from the income tax department alleging that they had failed to declare dividend income. According to Mr. Lasalle, these demands for payment, (allowing a very short time to reply), were often in error. For example, one taxpayer was being assessed for dividends paid into his tax-sheltered Registered Retirement Savings Plan!

The scary part is that the tax department is unable to produce a paper copy of the T5 form, which is normally sent to the taxpayer by his financial institution. Missed dividend declarations are determined on the basis of information transferred from the financial institution to the tax department. If a taxpayer has failed to keep records of previous taxation years (at least 3), he could end up paying more tax than he should to avoid trouble.

Peter Jones MAINT@UQAM (514)-987-3542

---

### **✂ Re: Another intrusive database ... ([RISKS-9.42](#))**

*Jim Horning <horning@src.dec.com>*

*14 Nov 1989 1514-PST (Tuesday)*

I'm surprised that people find this surprising. I moved from Toronto, Ontario to Palo Alto, California in 1977, and a couple of years later received a letter from the IRS asking me to account for income that appeared on my Canadian income tax return that they couldn't identify on my US return. (Fortunately, I was able to show that I had properly reported it). Ever since, I've assumed that transnational exchange of income tax data was routine.

Jim H.

---

### **✂ Re: Computer errors and computer risks (Davis, [RISKS-9.40](#))**

*David Smith <dsmith@dcsc.dla.mil>*

*Wed, 15 Nov 89 09:55:12 -0500*

Randall Davis suggests that using the terms "computer errors" and "computer risks" when speaking of social risks not arising uniquely from but only amplified by the use of computers leads to discussing these matters in the wrong forums -- computer technology instead of social morality. He says that, for example, if the misuse of computer databases and telecommunications to

implement policies that impinge drastically on individual privacy rights were truly a "computer risks" problem, all that would be needed to solve it would be the elimination of the computer.

It isn't quite that simple. The motivation to establish and implement a policy may exist, but if there's no tool to implement it adequately, the motivation will likely remain dormant, the policy unpursued. Only when a tool becomes available that makes implementation feasible will the policy be elaborated and implemented. It's possible to maintain large, irresponsibly constructed paper databases on suspected child molesters, but not feasible; with computers, it's not only feasible but easy -- the technology empowers the idea.

The existence of the motivation is a social moral concern. That the pursuance of policy based upon the motivation has been made feasible by the existence of a powerful and compliant technology is both a social moral concern and a technology concern. The distinction is important, but it shouldn't prevent discussion of the issue in both forums.

---

**✂ Re: Computer errors and computer risks (King, [RISKS-9.42](#))**

*John Locke <jxxl@cs.nps.navy.mil>*

*15 Nov 89 21:53:05 GMT*

In the incipient stages of their White House investigation, Woodward and Bernstein finagled access to a large quantity of Library of Congress records on books checked out by White House offices. The distillation of their findings was that E. Howard Hunt had done a massive amount of research on Senator Ted Kennedy, presumably to aid in smearing him should he decide to run for the presidency. The findings became part of a larger pattern of shady campaign practices.

This invasion of privacy seems palatable since, in the light of history, it can be deemed a "good cause." I could trivialize my next point by saying that a good laptop PC would have saved Woodward and Bernstein a couple of long evenings. But the fact is this, in the information age the widespread use of PC's serves as a kind of "people's revolution." Previous to PC's, computerized information processing was centralized and primarily accessible to a managerial elite. With the advent of PC's information processing capability has been decentralized to some extent. The possibilities for using computers to monitor government and business should not be overlooked.

---

**✂ Altered bit position in [Risks 9.39](#)**

*<sullivan@math.Princeton.EDU>*

*Wed, 15 Nov 89 19:36:25 -0500*

I get my news from phoenix.princeton.edu, and on that machine, [RISKS-9.39](#) arrived after 9.40 and 9.41. Furthermore, many characters had been altered, having their 2<sup>nd</sup> bit set. The most common changes were ' ' -> '\$' (happened 30 times) and 'h -> l' (there were many instances of the word "tle"). I also noticed y->}, s->w, i->m, p->t, b->f, r->v. Note that in all of these cases,

the letter substituted has ascii value exactly 4 greater than the original (one extra bit set).

John M. Sullivan Princeton Univ. Math Dept. [sullivan@math.princeton.edu](mailto:sullivan@math.princeton.edu)

[Similar behavior was reported by several other recipients, including [henk@cs.eur.nl](mailto:henk@cs.eur.nl) (Henk Langeveld) in Rotterdam, whose return path to me was "euraiV1!eurtrX!hp4n!mcsun!uunet!seismo!ukma!tut.cis.ohio-state.edu!gem.mps.ohio-state.edu!usc!ucsd!ames!!!!-lcl!unisoft!mtxinu!ucbvax!CSL.SRI.COM!risks". But his copy had an interesting FROM: field -- "From: rmsks@CSL.SRI.COM (RISKS Forum)".

We have reported previously on compression screwups making systematic substitutions. This one looks like a transient hardware bit error in the 4's bit, somewhere along the line. Before u4ia sets in, I hope someone can track down its origin. 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 9: Issue 44**

**Friday 17 November 1989**

## Contents

- [More on BART's new computer system](#)  
[PGN](#)
- [Computer misdirects phone calls for TV programme](#)  
[Olivier Crepin-Leblond](#)
- [Murphy's Law Meets the Navy](#)  
[PGN](#)
- [Unwanted Credit](#)  
[Stuart Bell](#)
- [Saskatchewan shuts down translation project](#)  
[Peter Jones](#)
- [Re: Another intrusive database with associated privacy problems](#)  
[Brinton Cooper](#)
- [Re: Are you sure you declared ALL your dividends?](#)  
[Jim Frost](#)
- [Re: L.A. Times "computer" problems \[anonymous\]](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **More on BART's new computer system**

*"Peter G. Neumann" <neumann@csl.sri.com>  
Fri, 17 Nov 1989 10:13:21 PST*

Last Saturday's San Francisco Chronicle article by Harre Demoro (summarized in [RISKS-9.41](#)) concerning BART computer troubles was apparently based on a partial simulation with only 10 trains and with intentional performance degradation resulting from the presence of trace software being used during a special-purpose test. That data was extrapolated to give the cited numbers. Also, the intended maximum number of trains was given incorrectly, and should have been 74 instead of 108. Thus, it appears that the article should be taken with a grain of salt.

The first real test to measure performance was conducted for eight hours, ending last Saturday morning -- after the article appeared. Dr. Norman Zachary, President of Logica Data Architects Inc. (the Logica subsidiary

responsible for the BART software), said on 15 November that "The results of the performance test conclusively show that Logica's system meets BART's specifications, including the ability to operate 74 trains automatically. We currently estimate we are very close to delivery of the system." (BART currently operates no more than 45 trains, but intends to go to 74 as part of its capacity expansion program.)

This update is based on several phone calls with BART and Logica people. Stay tuned for any later developments. Peter

---

### **✂ Computer misdirects phone calls for TV programme**

*Olivier Crepin-Leblond <zdee699@elm.cc.kcl.ac.uk>*

*Thu, 16 NOV 89 13:44:29 GMT*

Cricket is our equivalent of baseball in England.

Taken from ORACLE Teletext TV News Service, 2:00am, 16 NOV 89

"Yorkshire cricket fans were hit for six [ that's six runs... - OCL ] when they were invited to take part in a Yorkshire TV phone-in and received sex advice instead. After a programme called 'What's to do about Yorkshire Cricket', viewers were invited to ring a special number to give their opinions. But when they dialled, they heard a recorded message from 'Barbara' about sexual problems.

British Telecom (BT) blamed a computer fault... "

No comment.

Olivier Crepin-Leblond, Computer Systems & Electronics,  
Electrical & Electronic Eng., King's College London, UK.

[Also noted by Tim Steele <tjfs@tadtec.uucp> ]

---

### **✂ Murphy's Law Meets the Navy**

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

*Wed, 15 Nov 1989 18:27:43 PST*

The Navy has an elaborate safety program that includes extensive concern for safety in software-controlled systems. Unfortunately there is an apparent gap between the intent and the execution. (It will be interesting to see how much the Navy's two-day reorientation period designed to increase awareness actually helps.) For the record, here is a summary of the past weeks. It may be worth noting that none of this run of problems seems to have been blamed on computers (as far as I know), but then most of our so-called "computer problems" are people problems anyway, irrespective of where the blame is placed.

29 Oct. Pilot's first-ever carrier landing kills 5 on carrier Lexington.

30 Oct. FA-18 pilot drops 500-pound bomb on guided missile cruiser Reeves;

5 injured.

31 Oct. Wave washes 3 sailors overboard on carrier Eisenhower;

2 rescued; several dozen missiles lost.

31 Oct. 12-foot swells on carrier Vinson, sailor swept overboard, lost.

1 Nov. Boiler room fire on oiler Monongahela, 9 suffer smoke inhalation.

9 Nov. A-7E Corsair 2 crashes into apartment complex in Smyrna GA.

2 killed, 4 injured.

11 Nov. Destroyer Kinkaid collides with merchant ship.

1 sailor killed, 5 injured.

11 Nov. Two A-6 attack bombers dropped bombs near a capsite. One injured.

14 Nov. Amphibious assault ship Inchon catches fire in Norfolk, 31 injured.

14 Nov. F-14 Tomcat fighter crashes at sea, FL training flight, no injuries.

(Source: San Francisco Chronicle, 15 November 1989, p. A4)

---

## **✂ Unwanted Credit**

*Stuart Bell <stu@mwvm.mitre.org>*

*Thursday, 16 Nov 1989 14:25:58 EST*

Several months ago, an alcoholic relative applied for a credit card in his and my name - without my authorization. Eventually he began drinking and failed to intercept the bill when it arrived at my home. I immediately called the 800 number, cancelled the card and followed up with a registered letter.

Now the problems begin.

They sent me a follow up letter that indicated the balance had grown from \$1200 when I cancelled the letter to somewhat over \$2000. I called them and was informed that their computer was unable to cancel credit cards and was not programmed to refuse charges.

In the registered letter that followed, I informed them that I would pay the original \$1200 - even though both they and I agreed I was not responsible for this money. I declined to pay any further charges and told them there was no chance to recover the money from by relative - he was in a rehab center with no income.

They responded by encouraging him to declare bankruptcy - since that was the only entry their computer would accept to cancel a credit card. Amazed, I tried to explain to them about fair credit laws and such (I am not a lawyer but the concept isn't too difficult to understand). Eventually they agreed that neither he or I was responsible for the charges - but they still couldn't cancel the credit card - only put it in a warning bulletin in case someone bothered to look it up.

About the time the bill reached \$3000, they sent him a supply of pre-authorized checks to write against his credit limit. Another phone call prompted the response that neither he or I was responsible for any charges incurred by writing these checks - but their computer has no way to stop sending these out once we are entered into the database.

Eventually, the supervisor I spoke with began to understand the social responsibility of not giving unlimited funds to a drunk - was very sorry - but had no way to instruct the computer to stop sending out the credit cards (presumably he will get a new one when the current one expires) and the checks.

I sent a registered letter to the president of the bank offering some computing consulting to help fix their computer systems.

Any takers if he replies? The letter was acknowledged by receipt - but has caused no action from the bank. /Stu Bell

MS=NASA (713) 333-0906 STU%MWVM.MITRE.ORG

---

### **⚡ Saskatchewan shuts down translation project**

*Peter Jones <MAINT@UQAM.bitnet>*

*Fri, 17 Nov 89 08:13:19 EST*

According to a national newscast by the CBC at 7:00 EST, the Saskatchewan provincial government has decided to abandon the project to translate its laws into French using a computer system. This system was supplied by Guy Montpetit, who was also involved in LOGO Systems here in Montreal. The NDP opposition party had been criticizing the government for not checking into Mr. Montpetit's track record. (See "Gigatext Translation Services Inc. scandal" by Bhota San in [RISKS-8.84](#) for a lengthy report on this project.)

Peter Jones MAINT@UQAM (514)-987-3542

---

### **⚡ Re: Another intrusive database with associated privacy problems**

*Brinton Cooper <abc@BRL.MIL>*

*Thu, 16 Nov 89 13:56:08 EST*

Bill Gorman writes about "a treaty to detect and combat tax evasions on both countries. By means of this treaty both nations will have access to information concerning the income of mexicans living in the States and of northamericans living in Mexico."

It may be even worse than inter-governmental data sharing. More and more governmental functions are now being performed by contractors. (By using contractors, the US Government doesn't incur "entitlement" expenses such as pensions, injury/accident compensation, unemployment insurance, etc.) So, not only would the Mexican government have your tax history, but so would some contractor such as TRW or another "data basing" corporation that may already have access to your medical and credit histories. The possibilities are boundless.

Brint

---

### **⚡ Re: Are you sure you declared ALL your dividends?**

*jim frost <madd@world.std.com>  
Thu, 16 Nov 89 18:10:52 GMT*

On a similar note (Jones, [RISKS-9.43](#)), a few years back I wrote a system to be used by a bank to do electronic submission of 1099 forms (and some other similar forms). Shortly after submitting the forms, the bank received a letter from the IRS stating that the submission contained errors, each of which was fined, to a total of \$65,000. The bank was upset.

The error was that I left the "alpha" field, which is supposed to be the taxpayer's last name, blank for businesses (it's kind of hard to determine the last name of businesses). This was exactly what the documentation said you were supposed to do if you couldn't determine the correct field value.

Apparently they didn't tell their DP department that...  
jim frost, software tool & die

---

### **✶ Re: L.A. Times "computer" problems**

*<[anonymous]>  
Wed, 15 Nov 89 18:48:00 [X]ST*

Actually, since the database showed that the subscriber was only supposed to be receiving the Sunday edition, it is most probably the case that the daily deliveries were the result of a "lazy" newspaper delivery person, not the computers.

It is quite common for these folks, especially in metro areas where they drive by and throw papers rapidly at many houses, to not want to bother differentiating between people with different types of subscriptions. So instead of paying attention to the computer generated lists of who should get what, they just throw a paper at every house that EVER gets a paper, regardless of the list.

Sometimes it's even worse than that. For years we received our metro paper every day, without fail, even though we didn't have ANY subscription to the paper and called numerous times to try stop it. We weren't on any subscription lists. Apparently the delivery folks found it easier to just throw a paper at every house in the area instead of keeping track of the lists. One can assume relatively few people ever complained.



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

**Volume 9: Issue 45**

**Monday 20 November 1989**

## Contents

- [Another foretaste of the Millenium](#)  
[Brian Randell](#)
- [UNIX EXPO Blackout](#)  
[Brian Randell](#)
- [Autodialing horror stories](#)  
[John](#)
- [Self-trust and computer professionals](#)  
[Sean Eric Fagan](#)
- [Bit problem with RISKS-9.39 was more global](#)  
[Dan Johnson](#)
- [Gauge Proposed on Filing of Wage Data by Computer](#)  
[David B. Benson](#)
- [Congress Finds Bugs in the Software](#)  
[David B. Benson](#)
- ["Computer risks"](#)  
[Randall Davis](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **Another foretaste of the Millenium**

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

*Fri, 17 Nov 89 9:17:33 BST*

We apologise for the unexpected system shutdown today (Thursday). This was caused by a bug in the MTS system that was a "time-bomb" in all senses of the word. It was triggered by today's date, 16th November 1989.

This date is specially significant. Dates within the file system are stored as half-word (16 bit) values which are the number of days since the 1st March 1900. The value of today's date is 32,768 decimal ('X'8000' hexadecimal). This number is exactly 1 more than the largest positive integer that can be stored in a half-word (the left-most bit is the sign bit). As a result, various range checks that are performed on these dates began to fail when the date reached this value.

The problem has a particular interest because all the MTS sites world-wide are similarly affected. Durham and Newcastle were the first to experience the bug because of time zone differences and we were the first to fix it. The American and Canadian MTS installations are some 4 to 8 hours behind us so the opportunity to be the first MTS site to fix such a serious problem has been some consolation. The work was done by our MTS specialist who struggled in from his sick bed to have just that satisfaction!

[I presume the MTS folks did not read [RISKS-9.28](#), "Hospital problems due to software bug", in which we learned that 19 Sept 89 was 32768 days after 1 Jan 1900! Does that sound familiar to you?  
"When will they ever learn? ..."  
("Where Have All the Flowers Gone?") PGN]

---

## **UNIX EXPO Blackout**

*Brian Randell <Brian.Randell@newcastle.ac.uk>  
Fri, 17 Nov 89 11:03:04 BST*

I do not recall seeing anything in Risks about the incident described in the following front page article in the Nov 16 issue of (UK) Computer Weekly. It is here in full, as an amusing example for US readers of British "journalism".

### UK FAULT TOLERANCE SHINES AFTER US BLACKOUT

Jon Kaye

A fault-tolerant team from the UK has scored a valuable away win in New York despite strong opposition from the local favourites.

IMP, a manufacturer of fault-tolerant Unix machines based on Motorola's 68030 processors, beat top US firms Tandem and Sequoia during last month's Unix Expo.

On the final day a power cut left the exhibition centre without electricity for half the day.

Quick-thinking Dick Penny, IMP's marketing manager, weaved his way into Tandem and Sequoia territory, lobbying offers for a competition once the power returned.

"I thought it would be a good idea to see which machine would be up and running first once the power was back on," says Penny.

Tandem and Sequoia agreed, the latter "reluctantly", Penny says. The referee was provided by Unix International, the Unix standards group, setting the stage for an exciting kick-off.

The plucky UK lads were first to the goal in 70 seconds, followed by Tandem in two minutes and Sequoia in four.

Penny denies suggestions that IMP caused the blackout itself to get the competition staged. "Four city blocks went out", he says. "Organising that would have overstretched our marketing budget for the show."

Brian Randell, Computing Laboratory, University of Newcastle upon Tyne, UK

---

### **✂ Autodialing horror stories**

*<john@anasaz.UUCP>*

*Sat, 18 Nov 89 10:20:56 -0700*

I thought I would relate a couple of horror stories about a hotel reservation system that we implemented at Ramada Inns in 1974.

... A lady in Utah started getting anonymous phone calls in June, 1974. She would answer the phone and hear nothing. Sometimes, if she kept asking who was there, she would hear a loud screech before the caller hung up. Calls would come at all times of day and night, but were most frequent between 1 and 2:30 AM. The phone company tried to trace the calls, but they were of very short duration. They did determine that the calls were coming from area codes all over the US, with a random distribution. They were puzzled.

Meanwhile, a number of Ramada franchisees complained that they were getting billed for long distance calls on the phone line they had installed for their new reservation system computer.

We investigated and discovered that there was a phone number that was one dial pulse (there were lots of pulse-dial only exchanges then) away from the 800 number that the computers were supposed to call. We called the number and discovered on very frustrated lady! Ramada payed for her to get a new phone number, and the problem went away.

.... Also in June, 1974, there were long distance telephone outages occurring in the middle of the night, every night, in the Omaha, Nebraska, area. It turns out that our 700 computers were all calling in in a very short period of time after 0100MST, jamming the circuits. At 0100, our system started a period (called End of Day) during which the computers called in rapidly to unload their message queues. I had guessed at the number of lines, put it in a configuration file, and forgotten about it. I had guessed 20 lines. There were in fact quite a few less (I think there were 7). Thus the calls were coming in at a rate way to high to be serviced. To make it worse, a failed call was retried three times! The problem was corrected by changing the constant in the configuration file.

---

### **✂ Self-trust and computer professionals**

*Sean Eric Fagan <sef@kithrup.COM>*

*Sat, 18 Nov 89 18:29:48 PST*

After reading all the recent slate about computer-controlled everything (cars,

planes, trains, etc.), I realized something interesting: a layperson generally doesn't trust computers because he or she doesn't understand them (they are "black boxes"). A computer professional, on the other hand, doesn't trust them \*because\* he or she \*does\* understand them (and their limitations). This also lead me to realize that ours is one of the few fields where we wouldn't necessarily trust our "product" with our lives. That is, doctors generally will trust other doctors to operate on them, auto designers probably drive cars (8-)), etc. Yet, a programmer probably wouldn't trust a computer-controlled plane or car very much (for good reason, in my opinion). I'm not sure exactly what this says, except that it is still a very immature field.

Sean.

---

### **✂ Bit problem with [RISKS-9.39](#) was more global**

*Dan Johnson <dwj@acd4.UUCP>*

*Fri, 17 Nov 89 19:03:16 EST*

The problem that was experienced by some on [RISKS-9.39](#) was not limited just to comp.risks. There has been a recent discussion in news.admin about similar problems in other postings. In particular <10668@claris.com> and <1989Nov13.230546.8399@psuvax1.cs.psu.edu> isolate the problem to Ill-lcc and mention the munged [RISKS 9.39](#). Btw, we got a good copy and a bad copy of it (which arrived after 9.40 and 9.41); one of the bits hit was in the message ID, so the two copies travelled independently.

Daniel W. Johnson, Applied Computing Devices, Inc.

[Also noted by a variety of others... Thanks for all the examples. PGN]

---

### **✂ Gauge Proposed on Filing of Wage Data by Computer**

*David B. Benson <dbenson@cs2.cs.WSU.EDU>*

*Sat, 18 Nov 89 16:48:19 PST*

[The Wall Street Journal, Novemeber 17, 1989, p. A16]

WASHINGTON -- The Social Security Administration announced proposed standards for employer's computerized filing of wage data and said it might establish a certification process for software programs that comply.

The software standards are designed to reduce discrepancies between Internal Revenue Service tax data and Social Security wage data by requiring software programs to check for inconsistencies. This would help ensure full credit to 130 million American workers. The Social Security Administration routinely cross-checks data with the IRS. Improperly reported wages often result in workers receiving less than their entitled Social Security benefits.

Each year, in as many as a million cases information reported to the IRS fails to match that reported to Social Security, said Norman Goldstein, the administration's chief

financial officer. He estimated that computer software is used for filing the wage data of 70% to 80% of U.S. workers.

The proposed standards are voluntary, but Social Security Commissioner Gwendolyn King said she would like to see the draft proposal become the official U.S. standard. The administration is seeking comments on the software standard from business groups and software writers.

---

## ✂ Congress Finds Bugs in the Software

David B. Benson <[dbenson@cs2.cs.WSU.EDU](mailto:dbenson@cs2.cs.WSU.EDU)>

Sat, 18 Nov 89 17:39:32 PST

[AAAS Science, 10 November 1989, vol. 246, p. 753]

[by M. Mitchell Waldrop]

Dig into any of the government's chronically over-budget and behind-schedule development programs -- the Hubble Space Telescope of the B1-B Bomber, for example -- and you'll find that a good fraction of what gets labeled as "waste, fraud, and abuse" actually stems from crummy software. Not only do the development agencies habitually spend millions of dollars on operations software that is buggy, inadequate, and late, they have to spend millions of dollars more to fix it.

So says a just released report [nb. "Bugs in the system: Problems in federal government computer software development and regulation"(Subcommittee on Investigations and Oversight of the House Committee on Science, Space, and Technology, Government Printing Office, Washington, D.C., September 1989).] from the House Science, Space, and Technology Committee's Subcommittee on Investigations and Oversight. Written by subcommittee staffer James Paul, who spent 2 years working on it, the report also names a culprit: the government itself. "Government policies on everything from budgeting to intellectual property rights have congealed over time in a manner almost perfectly designed to thwart the development of quality software," it says.

Paul's brief, but strongly worded report echoes the complaints that computer scientists have been muttering for years. "The [federal government's] procurement process is as much or more to blame for poor software as any other single thing," says Peter Freeman of George Mason University, who just finished up a stint as head of the computer research division at the National Science Foundation. "There are huge numbers of people involved [in the agencies] who fundamentally don't have the knowledge or experience to make good decisions with respect to procurements."

The report says that reform must begin on the conceptual level, because purchasers still regard software as an afterthought. Project managers, agency heads, and congressmen alike tend to focus on sexy hardware such as radars, airframes, and engines, assuming that the software to control all this gadgetry can be taken care of later. Yet that assumption can be costly. In 1979,

the Nuclear Regulatory Commission shut down five nuclear reactors for upgrading; a software flaw in the computer-aided system used to design them had left them vulnerable to earthquake damage. In the mid-1980s, a Canadian-built radiation therapy machine, the Therac-25, killed at least four people when a software error irradiated patients with massive overdoses.

"Software," says the report, "is now the choke point in large systems."

On the other hand, it will be difficult to make the software development process more flexible because the federal procurement system effectively demands that contractors write the software using bad methodology. "Out on the technical frontiers," the report says, "the government requires a legally binding contract specifying in excruciating detail exactly how the system will look at delivery some years hence." The tacit assumption is that programmers will then use the specifications to write, test, and debug the software. In the programming community this approach is known as the waterfall model because the work supposedly cascades from one stage to the next in systematic progression.

But modern programmers consider the waterfall approach an abysmal way of doing things. Especially when it comes to high-tech systems such as the Space Telescope's scheduling software or the B1-B's defensive electronics countermeasures systems -- both of which were software fiascos (Science, 17 March 1989, p. 1437) -- it is essentially impossible for anyone to write detailed specifications in advance. Not only does the hardware evolve during development, thereby forcing the specifications to change, but the hardware engineers themselves have no way of knowing what they really want from the software until they have had a chance to try it out.

This is why the modern "evolutionary" approach to software development looks less like a waterfall than like a spiral. Starting with general requirements, the programmers quickly cobble together one or more prototype systems. The engineers then try out the prototypes on the evolving hardware. Their suggestions guide the programmers in refining new prototypes. And the process repeats as long as is necessary. The payoff is that the programmers have a much better chance of catching errors in the design phase, when the bugs can be fixed at an estimated one-tenth to one-one hundredth the cost of fixing them after deployment, and the software as a whole has a much better chance of doing what it really needs to do.

But flexibility is precisely what the spell-it-out-up-front procurement culture lacks, says the report. In addition, the bureaucracy balks at the big up-front investment in problem definition that must be made when the evolutionary approach is used. Furthermore, as the report notes, "no program manager relishes the thought of defending a request for funds when the major activity seems to be endless arguments over abstruse technical points by large numbers of well-paid engineers."

So, what can be done? In the near term, very little, says the report.

The Department of Defense and a few other agencies have

begun to move away from the waterfall model, and Paul thinks those steps should be encouraged. Better methods should be developed for evaluating the quality, reliability, and safety of software, the report says. And perhaps the software community should be encouraged to establish some form of professional certification standards.

But nothing fundamental is going to change without changes in the procurement culture, says the report. And that is going to take awhile, even though chronic cost overruns and scandals are creating mounting pressures to do so. "Its not something you can jump right in and legislate," Paul told Science. "The federal procurement system is like a software system with bugs. Every time it's broken down, somebody has patched it. But keeping it together is getting harder and harder and costing more money. And at that point, an experienced software engineer would throw up his hands and say, 'Hey! Let's toss this out and start over.'"

---

## ✂ "Computer risks"

*Randall Davis <davis@ai.mit.edu>*

*Mon, 20 Nov 89 10:15:40 est*

Several people responded to my posting in 9.40 regarding "computer risks," and many of them seem to me to share the same fundamental confusion. Let me use Saltzer's response in 9.41 as a representative example. He replied

>I claim that it is not that simple. In a traditional library, it was possible  
>to invade your privacy by making a list of all the books you have every  
>checked out.

Sorry but I believe it is in fact EXACTLY that simple and indeed the example cited shows it to be so.

The crucial point is confusing the technology that makes an act feasible, with the act itself.

As Jerry pointed out:

> The speed and efficiency with which data can be processed by computer can  
> convert a negligible risk into one worth discussing.

Just so; it is now \*worth discussing\*. But \*what\* is it we should \*discuss\*?  
Privacy, not technology.

We ought to discuss whether records of one's book reading should in fact be public. True, the question never arose routinely before because it wasn't pragmatically possible ("benign protection by the status quo," in Ware's elegant phrase). Previously the question was moot, now it is worth discussing. But what ought we to discuss? The QUESTION, not the TECHNOLOGY that rendered it relevant. And question is, what rights to privacy ought I to have when I borrow books from a public library? That question (a social and moral concern, as Dave Smith points out) is the central issue in such

discussion.

That discussion will need to be INFORMED by technology to some degree: people need to understand that certain actions will become easy in a computerized book lending system that were difficult before (e.g., monitoring, compilations, cross-matching). But those actions are now EASY rather than HARD, not POSSIBLE vs UNIMAGINABLE.

On this point, Ware quotes Hamming to the effect that

> "when something changes by an order of magnitude, there are fundamental  
> new effects."

Perhaps, but it's important to understand that they are often new only in the sense that we did not think of them previously (in the old technology), not that they are incomprehensible or unimaginable in those terms. For example, monitoring, compilations, and cross-matching of library records are all possible now for enormous databases. But I can perfectly well understand them and their effects by imagining the corresponding manual operations.

That distinction in turn is very important because it empowers people. Admitting that there is nothing fundamentally new in such a system makes it clear that ordinary people (incredibly enough, even those without degrees in computer science) can coherently and intelligently discuss these issues based on their ordinary intuitions and feelings about privacy. It even makes it clear that if there is a relevant specialized experience for this discussion, it is probably constitutional law, not computer science.

It's time to take the veil of technological mysticism off these issues. And it is we in particular who ought to remove the veil. People need to understand that their existing knowledge, experience, and opinions on privacy (and other issues) are both relevant and sufficient for informed debate. The crucial decision is whether the information ought to be public, not how it is to be accessed.

As for the argument that:

> The Registrar of Motor Vehicles in Massachusetts has long used the "it has  
> always been public" argument on car registration information as an excuse for  
> selling tapes to mass mailers.

That's little more than a bad pun, playing off two meanings of "public". But perhaps we need a finer distinction to avoid being tripped up by it in the future, hence my use of the term "pragmatically possible". Neither the motor vehicle nor the library data were in fact ever pragmatically public, so the issue never arose. But now they can be and now we need to decide whether they ought to be.

And *that* decision has nothing to do with the technology that made the point worth discussing, and everything to do with our own sensibilities about privacy.

In a similar vein, David Smith suggests that

> if there's no tool to implement [a policy] adequately... the policy  
> [will not be] pursued. Only when a tool becomes available that makes  
> implementation feasible will the policy be ... implemented.

Right, and then we should discuss the POLICY, not the technology that made it worth discussing.

He also adds:

- > It's possible to maintain large, irresponsibly constructed paper databases
- > on suspected child molesters, but not feasible.

Perhaps he's not had much experience with: insurance companies, medical records, legal records, the early social security system, etc., etc. Large irresponsible paper databases have been with us a long time.

King claims that he

- > supports the original thesis that, for serious breaches of privacy,
- > lack of a computer is no protection against data collection.

True, lack of technology doesn't preclude serious breaches of privacy, hence to some degree we've always faced these issues. But that's not the point, and it wasn't the original thesis. Even if lack of computers DID prevent breaches of privacy, that would only render the point moot; it would not ANSWER the question. And the question is, what rights to privacy ought we to have.

One might say that computerizing the records will make possible invasions, hence it is a computer risk. But then in the same breath one ought to point out as King does that computerizing the records will make possible a unprecedented degree of privacy (just erase the disk packs; no one could erase all the records in each book every two weeks, another order of magnitude effect). Hence we ought also to talk about the computer benefit. Then, having established that the technology can be used both to invade and to ensure privacy, we ought to get back to discussing the real question: what kinds of privacy ought I to have?

Finally, Jerry indicated that he is

- > ... prepared to tolerate a certain amount of fuzziness in identifying the
- > edge of the computer-RISKS arena by our beleaguered moderator.

The message was to the multitudes, not the moderator. It is important that we all remove the illusions of mystery about this stuff. People need to be empowered to think about this on their own and we should be telling them that. We need to make it clear to them that what makes the issue worth discussing (the technology) is quite distinct from what the issue is (what rights to privacy ought we to have).



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 9: Issue 46

Wednesday 22 November 1989

## Contents

- ["Play it Again, Yonkers" -- more election funnies](#)  
[Steve Bellovin](#)
- [Army shuts down computers and goes home due to rain](#)  
[Rodney Hoffman](#)
- [More good news -- Privacy and risks in credit information](#)  
[Bill Gorman](#)
- [Automated Bank RISKS](#)  
[John Howard Osborn](#)
- [Another Foretaste of the Millenium? \(corrigenda\)](#)  
[Brian Randell](#)
- [Re: Self-trust and computer professionals](#)  
[Jerry Hollombe](#)
- [Re: Congress Finds Bugs in the Software](#)  
[Franklin Davis](#)  
[Bob](#)  
[David Gursky](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✉ "Play it Again, Yonkers" -- more election funnies

<[smb@ulysses.att.com](mailto:smb@ulysses.att.com)>

Mon, 20 Nov 89 21:54:59 EST

I held off submitting this in the hope that someone who knew the complete story would post it; that hasn't happened, so here's what I know.

There was a very close, and racially-charged, mayoral election in Yonkers, NY; the challenger was rather unexpectedly reported the victor by 4,000 votes on election night. When the official tally was started, though, the incumbent had picked up 1,500 votes in just 5 of the 12 precincts. The count was suspended for the weekend, with the voting machines impounded; when it was finished, the original result -- and numbers -- were upheld.

What happened? It's an old story here, I'm sure. Before the election, the

tally program was run with test input data. They forgot to take out the test data when tabulating the real returns. From the story I heard, it wasn't clear if the error was in the official tally or in the early returns; given the numerical result, I tend to suspect the former.

--Steve Bellovin

---

### **✂ Army shuts down computers and goes home due to rain**

*Rodney Hoffman <Hoffman.ElSegundo@Xerox.com>*

*22 Nov 89 07:52:30 PST (Wednesday)*

Roddy Stinson is a columnist for the San Antonio, Texas "Express-News". Here's one Question & Answer from his column of Nov. 14, 1989 under the headline 'RAINSTORMS DIDN'T STOP THE ARMY WHEN I WAS IN IT':

The complaint desk is open --

PLAINT: I am a retired Army sergeant. My wife just got out of intensive care at Brooke Army Medical Center. I tried to call BAMC to make a medical appointment for her, and this is the message I got: 'The patient appointment system cannot operate at this time. Due to inclement weather, the computers had to be taken down. Please continue calling periodically. Thank you. This is a recording.' That's pitiful. That's ridiculous. What happened to typewriters and phones? If a rainstorm can shut down the country, we're in big trouble. I'll tell you one thing -- rainstorms didn't stop the Army when I was in it. They told me to keep marching, and I did.

[Stinson:] A spokesman for BAMC explained: "This (computer shutdown) happens every time there is a possibility of thunderstorms because the central appointments system is linked to a mainframe a mile and a half away, and if lightning hits the lines, everything on there could be erased." When I expressed skepticism, he added: "Believe me, it has happened. Lightning takes out our phone system and electricity on a regular basis." Progress marches on.

---

### **✂ More good news -- Privacy and risks in credit information**

*"W. K. (Bill) Gorman" <34AEJ7D@CMUVM.BITNET>*

*Mon, 20 Nov 89 13:08:34 EST*

Upon doing a routine, periodic inquiry of the local credit bureau to make sure they have things reasonably straight on my credit report, I made a rather disturbing discovery. The report issued to me, and presumably to whatever business (or person representing themselves as a business) contains not only the expected credit information, but THE NAMES, CREDIT LIMIT, ISSUERS, AND CARD NUMBERS OF ALL MY CREDIT CARDS AS WELL! It might pay others on RISKS to find out if this sort of thing is SOP, or merely the result of the incompetence of our local bureau.

---

### **✂ Automated Bank RISKS**

*John Howard Osborn <osborn@cs.utexas.edu>*

*Tue, 21 Nov 89 14:41:21 CST*

My bank, First Interstate, has recently implemented a handy new service. Using any touch-tone phone, bank customers may get information about the status of their account at any time. Normally, to get an account balance, the customer must enter the amount of his latest deposit. This provides, I feel, at least some measure of security. The problem is that the system also allows merchants to check a check. That is, will a check, for a certain amount, from a certain account, clear at this time? There is no security for this procedure. The merchant simply dials, enters the single digit code "6 - Validate a check" from the vocal menu, enters the account number, and finally the amount. The computer will then return a boolean clear/no-clear. Computer Science students will recognize this for what it actually is: a medium for a binary search. (At this point I refer the interested reader to *\_Sorting and Searching\_* by Knuth.) The potential for abuse is obvious: Given the account number, it becomes trivial to find the account balance.

My only shock is that the designers of the system were so casual about the RISKS involved.

John H. Osborn, University of Texas at Austin Comp. Sci. Dept.

---

### **✦ Another Foretaste of the Millenium? ([RISKS-9.45](#), corrigenda)**

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

*Tue, 21 Nov 89 10:12:20 BST*

[Brian sent me two versions of the MTS saga, part of one of which ran in [RISKS-9.45](#) -- but without the explanation indicating that the MTS message was not from Brian but rather from someone else. The surrounding text is given below, in case anyone thought that the "We apologise ..." message was originally Brian's. I apology to Brian in case anyone was misled. PGN]

The university computing service here runs MTS (the Michigan Terminal System) on an Amdahl mainframe, which crashed mysteriously today, as did various other MTS sites in North America, some time later. The explanation is given in the following message which I have just received from one of the systems programmers here.

> We apologise for the unexpected system shutdown ... [see [RISKS.9-45](#) for text.]

I hadn't realised that there was this disadvantage to living on this side of the Atlantic! Ah, well, it makes up for various advantages :-)

Brian Randell

---

### **✦ Re: Self-trust and computer professionals (Fagan, [RISKS-9.45](#))**

*The Polymath <hollombe@ttidca.TTI.COM>*

22 Nov 89 02:49:58 GMT

}... A computer professional, on the other hand, doesn't trust them  
}\*because\* he or she \*does\* understand them (and their limitations). This also  
}lead me to realize that ours is one of the few fields where we wouldn't  
}necessarily trust our "product" with our lives. That is, doctors generally  
}will trust other doctors to operate on them, auto designers probably drive cars  
{(8-)}, etc. Yet, a programmer probably wouldn't trust a computer-controlled  
}plane or car very much (for good reason, in my opinion). I'm not sure exactly  
}what this says, except that it is still a very immature field.

One of my oldest friends is an anesthesiologist. She put off having a hysterectomy until she was nearly incapacitated because she knew all the things that could go wrong during the operation.

I'm a licensed aircraft mechanic (and pilot). If you knew what I know about mechanics you'd think twice about getting into an air liner (though I do fly when necessary). I stay away from helicopters, except for emergency situations, because I know just how complex and fragile they are.

I wonder how many other experts in life-critical systems could scare us with their specialized knowledge.

The Polymath (aka: Jerry Hollombe, hollombe@ttidca.tti.com),  
Citicorp(+)  
TTI 3100 Ocean Park Blvd., Santa Monica, CA 90405

---

## **✉ Re: Congress Finds Bugs in the Software**

Franklin Davis <fad@Think.COM>  
Wed, 22 Nov 89 11:47:37 EST

In [RISKS 9.45](#) David Benson quotes from a Science article by M. Mitchell Waldrop:

... But flexibility is precisely what the spell-it-out-up-front procurement culture lacks, says the report. In addition, the bureaucracy balks at the big up-front investment in problem definition that must be made when the evolutionary approach is used.

These two sentences seem inconsistent to me. What's the difference between "spell-it-out-up-front" detailed specifications, and a "big up-front investment in problem definition?" There's some fuzzy thinking going on here.

I agree that it is impossible to precisely specify a large software system when the hardware environment and functional requirements aren't frozen. In those situations it may be necessary to prototype the system in order to understand the problem.

But I don't believe the software development community has reached consensus about tossing out the waterfall method. My feeling is that it is our inability or unwillingness to document requirements and specifications rigorously that is the source of most fiascos. Maybe the government requires the wrong kinds of details in its specifications, and doesn't adequately review them for sanity.

How will switching from "specifications" to "problem definitions," and then hacking together a prototype which is then "evolved" solve any problems? This is the old method of software development that modern software engineering methods are trying to get us out of. Only if you throw away the prototype might there be hope you can then specify the system correctly.

--Franklin Davis      Thinking Machines Corporation

---

✂ [Risks 9.45](#)/Gov't bugs

<CES00661@UDACSVM.BITNET>

Tue, 21 Nov 89 07:43:45 EST

In [Risks 9.45](#) David Benson discusses bugs in government software and discusses some of the causes/reasons behind them. I'd like, some day, to actually see two notes in the forum at the same time in a scenario like: David discusses problems with detailed up-front procurement specs and someone else discussing the problems with less-than-complete procurement specs causing problems. It seems to be a no-win situation. Those up-front specs didn't come out of nowhere. They were Congress', watchdogs', politician's etc. attempts to solve a problem. In typical Congressional ways, they use atomic weapons to kill flies(!). Each line in those regulations was probably the result of some (comparatively) trivial screw up. It has since cost us multiple orders of magnitud more to "fix" the problem than to let it alone.

David's suggestion to abandon the waterfall approach to software design is good, but it carries the rather large risk that if it doesn't happen to work ONE TIME, you might get a "Golden Fleece" award and have your career dead-ended.

As an interesting aside, I found issue 9.45 to have more meat in it than many in a long time. David's discussion, and the discussion of technology vs. policy is what this forum needs more of. Maybe the recent chastisers have had a good effect. Thanks.

Bob

---

✂ **Re: Risks in RISKS???**

David Gursky <dmg@lid.mitre.org>

Tue, 21 Nov 89 07:37:31 EST

I noticed the following gem in David Benson's (dbenson@cs2.cs.WSU.EDU) posting about Congress finding bugs in software...

> the Hubble Space Telescope of the B1-B Bomber, for example ...

Now I neither do work on the HST, or the B1-B, but I know something of both systems. I would suggest to Congress, Mr. Benson, or the author of the AAAS article (which ought to know better), that mounting the HST on the B1-B (I would guess as a bomb sight, having no other conceivable purpose by my guess)

is, uh, overkill? ;-)

[The original \_Science\_ article by M. Mitchell Waldrop of course says  
"the Hubble Space Telescope or the B1-B Bomber, for example ..." 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 9: Issue 47

Friday 24 November 1989

## Contents

- [Air Force Radar Risk \(update\)](#)  
[Henry Cox](#)
- [Congressional report: "Bugs in the Program"](#)  
[Gary Chapman](#)  
[Dave Davis](#)
- [Re: Specifying vs. defining](#)  
[Dave Platt](#)
- [Training programmers](#)  
[Lee S. Ridgway](#)
- [Re: Privacy and risks in credit information](#)  
[John DeBert](#)
- [Re: Automated Bank RISKS](#)  
[Marc Shannon](#)  
[Jon Mauney](#)
- [Re: Autodialing horror stories](#)  
[Robert Sansom](#)
- [Info on RISKS \(comp.risks\)](#)

---

✉ [Air Force Radar Risk \(update\)](#) [See [Jon Jacky](#), [RISKS-8.28](#)]

*Henry Cox* <[cox@pike.ee.mcgill.ca](mailto:cox@pike.ee.mcgill.ca)>

*Thu, 23 Nov 89 10:20:29 EST*

RADAR AT U.S. BASE CAN TRIGGER PLANES' EJECTION SEATS: LETTER

[ From the Montreal Gazette, 23 November 1989 ]

Knight-Ridder Newspapers

Robins Air Force Base, Ga. - The US air force has learned that radiation from its PAVE PAWS radar at Robins AFB could activate internal equipment - including ejection seats and fire extinguishers - on virtually all planes that land at the base.

The disclosure was made in an Air Force "update" letter to Senator Sam

Null (D-Ga.) made public this week by the senator's Washington office.

Although the air force originally said that PAVE PAWS would not endanger electro-explosive devices other than those on the outside of its plane, a recent review of the radar has concluded otherwise, the air force letter said.

"As a result, Air Force Space Command is co-ordinating with the Air Logistics Center at Robins AFB to implement procedures to ensure aircraft with internal EEDs are also protected," wrote Maj.-Gen. Burton R. Moore, the air force's director of legislative liaison.

But Nunn, in a written reply to Moore dated Nov. 20, says that the air force hasn't fully answered his questions of last January, and has "raised new questions" with its latest update.

"It would be helpful to know more about the hazard to such devices, what the devices are used for, and what aircraft are equipped with them. I would also like to know how the air force determined that these devices were at risk," said the Senate Armed Services Committee chairman in his two-page letter.

The radiation hazard to internal EEDs is the latest safety revelation concerning the southeastern PAVE PAWS - built too close the runway at Robins AFB. The radar, one of four nationwide, is designed to warn of sea launched missile attacks and track satellites in space. But since November of 1987, the air force has been turning off the north face Robins PAVE PAWS to protect vulnerable planes landing on its runway 3 kilometres north of the radar.

According to air force documents obtained by Knight-Ridder Newspapers recently under the Freedom of Information Act, one aircraft at risk to PAVE PAWS is the Strategic Air Command's KC-135R tanker, some of which are based at the 19th Air Refuelling Wing at Robins.

EED equipment on other aircraft includes "flare/chaff dispensers, pylon/ejector racks, tactical missiles, cruise missiles, crew escape, and engine start cartridges," according to air force documents.

[This problem was noted in [RISKS-8.28](#), 19 FEB 1989. Details are new. PGN]

---

### **✂ Congressional report: "Bugs in the Program" [Benson, [RISKS-9.45](#)]**

*Gary Chapman <chapman@csl.stanford.edu>  
Wed, 22 Nov 89 12:06:19 PST*

I have a copy of the report David Benson's message referred to--the congressional committee report called "Bugs in the Program"--and I have some comments on its recommendations about software development.

There is an emphasis in the report--an overemphasis in my view--on the Federal procurement process for software. This is probably understandable given the source of the report; Congress is concerned about spending money, not about methodological issues in software engineering. However, the attention being given to this report, and its emphasis on the procurement process, could lead

to some misconceptions in the Congress about the nature of the problems we face.

The fundamental problem about emerging computer risks is that computer scientists are trying to integrate, in a systematic and predictable fashion, three domains: discrete state machines, the highly contingent and variable-rich nature of the "real world," and the equally unpredictable character of human subjectivity and intent. This is a project similar to that of Leibniz, for example, when he said that what philosophy should aim for is a mathematical calculus that would provide an equation for any question--in other words, absolute certainty for any aspect of experience, expressed in logical and mathematical evidence. Leibniz didn't succeed, and for the most part we don't take this kind of enterprise seriously anymore, except in developing complex computer systems.

Since the whole nature of the "software crisis" is really just a dilemma produced by the inability of people to adequately predict the future down to the level of detail required by computers and their ancillary equipment, it is something of a wonder why so many people are puzzled by the fact that we find ourselves in this conundrum, or why we're wasting so much money in this effort. Not to be too melodramatic about it, but the core of the Greek tragic tradition is a mortal protagonist trying to manipulate the world according to his designs, and then discovering, usually by running up against the wrath of the gods, the limits of human power. These days the gods deliver their lessons by burning up mountains of money.

There seems to be a cognitive block on the part of many people in the policymaking apparatus in understanding the real nature of the problem. The congressional report, for example, once again hauls out the various government reports on the Strategic Defense Initiative and its software problems, as though this idea was legitimate to begin with, that the whole thing is something more than just an embarrassing boy's fantasy of omnipotence in space, etc. The Congress continues to treat the SDI, and its software difficulties, as a real technical challenge, one that is only receiving less attention than previously because of budget problems and the changing nature of the Soviet threat. The report quotes the Defense Science Board when it said that the "The Strategic Defense Initiative. . . has a monumental software problem that must be solved to attain the goals of the initiative." This sentence makes one slack-jawed with amazement. Not only is it eye-rollingly obvious, but it harrumphs that this "software problem" is something to be solved, which by now should be considered completely absurd. As Jack Ruina of MIT once said, the SDI should have all the scientific credibility of astrology or water-dousing, so the sentence of the DSB quoted in the congressional report should have all the solemnity and relevance of a pronouncement on one's moon in Pisces. The fact that the SDI "software problem" is still discussed as a vexing issue of public policy and an example of the growing software crisis shows how far off the Congress is from understanding the true nature of the problem.

Another showcase example of the report is the B-1 bomber, and the citations about the B-1 are once again from government agencies, the well-known muckraking journal *Aviation Week & Space Technology*, and Jacques Gansler of MIT, who is not only famous for his sympathy to the Pentagon, but who also runs a private defense consulting firm. There are no references to Nick Kotz's book *\*Wild Blue Yonder: Money, Politics, and the B-1 Bomber\** (1988, Princeton

University Press), widely considered the definitive book on this fiasco. Kotz says, "After a continuous thirty-year defense buildup, marked by [such] repeated excesses, the military program is totally out of control." This context in which large software projects are developed is completely absent from the congressional report. The story of the B-1 is not a story of technical or procurement failures relating to its avionics software, although this is certainly part of the overall narrative. It is a sad and enraging story of mismanagement, overselling, congressional cowardice and laziness, and propaganda. "Improved" software procurement procedures would be nearly negligible in any real remedy to these problems.

The report by James H. Paul and Gregory C. Simon does provide a real service in that it alerts the somnambulist Congress to some of the problems with software safety, reliability, and professional education. But if the result of the report is to try and crack the whip on the software engineering profession in order to produce more efficient development of code for the SDI, or for the B-1 bomber, or any number of projects that are doomed for entirely exogenous reasons, the report will be regrettable. The report recommends professional certification, for example, which is an issue that I have not developed a position on, but it seems to me completely premature to be talking about professional certification for software professionals when the Pentagon itself is a runaway train, and largely due to Congress' gullibility over high tech funding requests. It seems comic and slapstick if the Congress has overseen a project like the B-2 bomber, for example, on which we have spent \$22 billion, and then is alerted by the Pentagon that this aircraft will cost somewhere around half a billion dollars per copy, which puts Congress into a swirling faint all of a sudden--and then when Congress recovers it shakes a wagging finger at software engineers? Or after spending \$16 billion on SDI research, Congress lethargically asks, how much will the software cost for this thing, and the answer is eighty-eight kigillion dollars and the lifetime careers of every single programmer in the Free World (which appears to be expanding). And Congress says, years into this thing, What??!! Why weren't we told? Let's see a report on professional certification and the ethics of this profession! Give us a break! The SDI was wasting money when it was just an idea in a paid official's head, if he was thinking about it during working hours.

So it seems disingenuous to me, even if the intent was noble, to produce a congressional report that quotes approvingly the following passage: "Education is the seedbed of good practice. Whether computer science education in American universities is contributing to or inhibiting good software practice is not clear. . . ." There is the clear call for "professionalization" of the software field, and for the weeding out of incompetents and unethical bad apples. This from an institution that is a nonstop geyser of money for crackpot ideas and mismanagement, money that will of course be willingly deposited by people who are "professionals" at taking government money. Congress, in a bar wearing a suit bulging with cash, and willing to listen to every customer with a harebrained scheme for a big expensive system that will save the world from disaster, is growling and spoiling for a fight when it finds itself on the street wearing nothing but boxer shorts. The "cautiousness" of Congress in getting religion about software reliability and cost overruns starts to look pretty silly, like one of the rich, pompous and street-stupid louts that the Marx Brothers were always taking to the cleaners.

Gary Chapman  
Executive Director, Computer Professionals for Social Responsibility

---

**🔥 House report on software development and regulation [another view]**

*USENET NEWS <news@linus.mitre.org>  
22 Nov 89 20:38:49 GMT*

The House Committee on Science, Space, and Technology has just published a new comprehensive report on software development, government procurement, and user safety risks called Bugs in the Program. The cause of the study was the Therac-25 X-ray therapy system, which has been discussed elsewhere [in RISKS]. The well-researched report describes some of the reasons for a software crisis, citing inadequate technical capability to predict reliability and safety as causes of accidents due to software. In addition, it points out that all government agencies have difficulty in managing complex software development due to lack of technical and management training and experience. Also, inadequacies in computer science education and ethical training in our profession are noted.

The rigid hardware approach to procurements and development is criticized as being inappropriate to software, the most flexible part of systems. (One almost forgets this after living with these standards for a few years.) Prototyping and user interaction during development is recognized as promoting success.

The report recommends that Dr. Demming's statistical process control methods be applied to software development and testing. Further, it recommends that a Working Group be established under the committee to begin improving the software development process within the government, with assistance from NASA. More research into future software problems and solutions should be funded, and the government should develop the capability to evaluate proposed improvements in the development process.

Dave Davis, MITRE Corp., McLean, VA

---

**🔥 Specifying vs. defining (Davis, [RISKS-9.46](#) on Congress, [RISKS-9.45](#))**

*<dplatt@coherent.com>  
Wed, 22 Nov 89 15:44:13 PST*

> These two sentences seem inconsistent to me. What's the difference  
> between "spell-it-out-up-front" detailed specifications, and a "big  
> up-front investment in problem definition?" There's some fuzzy thinking  
> going on here.  
>  
> I agree that it is impossible to precisely specify a large software  
> system when the hardware environment and functional requirements aren't  
> frozen. In those situations it may be necessary to prototype the system  
> in order to understand the problem.

I believe you've hit the nail on the head in your second paragraph, and in effect answered the question you raise in the first.

The "spell-it-out-up-front", detailed-specification approach attempts to spell out THE SOLUTION in great detail. For example, the contract might call for a microprocessor-based implementation using a distributed network of FooBaz 413 MPUs, running a real-time operating system capable of responding to interrupts in no no more than 0.8263 nanofidgets, and capable of processing 1763 meta-shift-cokebottle commands per cup of coffee.

These sort of solution-specifications are often very comforting to the contract-writer... they provide a detailed, measurable, and testable description of the solution which must be delivered. When the project ends, it's relatively easy to compare the solution-as-specified with the solution-as-delivered, and see whether there are any shortfalls.

This is all fine... as long as the person writing the specification *\_really\_* understands what the problem is, and is actually capable of specifying a package which will solve the problem. If so, everybody's happy.

However... as others have pointed out, the solution is often specified well before the problem is really understood, or by people who aren't as aware of the problem as they should be. The net result is a situation we've seen all too often... a solution is delivered, it meets all of the project specifications, and yet proves to be inadequate when actually tested in the field, or to be incompatible with other packages it really *\_should\_* work with, or...

Things can get much worse... if, for example, the specification is changed part-way through the project. Adding a new requirement or two to the specification can throw the whole implementation effort entirely out of joint... leading to schedule slippage, cost overruns, or a patchwork solution that proves to be unmaintainable. All too often, the solution must be thrown away, and a new one developed at great expense... often by the same process, alas.

To paraphrase a guy I work with: "Don't hire me as a designer, and then tell me what to implement. If you do, you've just done my job, and you don't need me. Instead, tell me about your problem."

Dave Platt, Coherent Thought Inc., 3350 West Bayshore #205 Palo Alto CA 94303

---

## **✂ Training programmers**

*"Lee S. Ridgway" <RIDGWAY@mitvma.mit.edu>  
Wed, 22 Nov 89 13:37:24 EST*

Given recent discussion about programming and programmer standards, and the kind and quality of training programmers do or should get, I noticed (and pondered the implication of) an ad on the Boston subway for a trade school (CPI) in Cambridge, Mass., that announced the following training schedule for four computer-type jobs:

Computer Operator - 20 weeks  
Computer programmer - 12 weeks  
Computer technician - 7 months  
Data entry operator - 20 weeks

Seems a tad short time in which to learn programming with any depth or proficiency, except maybe Basic. Would any of you, in the position to do so, risk hiring an entry-level programmer from such a training program?

The school claims a 97% (overall) placement rate for its grads. Nothing about accreditation, or enrollment requirements, etc. Too bad all the little tear-off info cards had been torn off.

---

**✂ Re: Privacy and risks in credit information (Gorman, [RISKS-9.46](#))**

*John DeBert <onymouse@netcom.UUCP>  
24 Nov 89 07:15:57 GMT*

TRW lists all information received from their customers, or, clients, as TRW calls them, I believe.

This info includes the name of the client, your account number with them, the type of account, the balance, balnce past-due, who has requested your credit history and personal information such as social security numbers, your residence addresses for at least the past few years as well as personal information on whomever uses your credit accounts.

TRW also has a program called TRW Credentials Service which you may subscribe to. For thirty-five dollars per year, you can get your credit record that is on file with them. They also send you forms to fill out and return to them that - if you fill them out completely - contain a complete and current financial profile of you and your family. This information is kept online along with the regular credit file and is made available "only upon application and with your PIN code, which you provide the person or agency which would request it."

There are some really serious privacy problems with this service. Of course, TRW is still a popular target for crackers and it is used by government, businesses, et cetera, looking for information. I have asked TRW to tell me who would have access to my records without my knowledge and they have thus far not only refused to make a reply but never, ever answer any written request for information that I make. (TRW also says that they will notify me anytime someone requests a copy of my credit report but have failed to do so: I have received an updated report in response to sending them a correction to it and it shows some inquiries that were never reported to me.)

jd

---

**✂ Re: Automated Bank RISKS (Osborn, [RISKS-9.46](#))**

Marc Shannon <SYNFUL@DRYCAS.CLUB.CC.CMU.EDU>

Thu, 23 Nov 89 14:55 EST

My bank had implemented a Telephone Banking service a couple of years ago, but their implementation of security is a bit better. To get in, you enter the last ten digits of your ATM card and then your four-digit PIN code. Once in, you can check your balance, inquire on check status (by check number) or a recent check history, last deposit, transfer funds between accounts, and even pay bills.

The only problem I've ever had with it is occasionally I'll enter \*SOS# to talk to a Customer Service Representative, get the voice message (with annoying pauses: "Please . hold . on . and a . customer . service . representative . will . assist . you!" (note that there is no pause between "and a" :-)). Then a click, and then a dialtone! After hitting a key on the phone to see what it would do, I get transferred back to the telephone banking service. Isn't that special! :-)

(Customers can go directly to the representatives by entering a different menu code before going to the telephone banking service. If they try and ask for any information on an account, the representatives will have them go back to the service and enter their 10 and 4 digit codes for security.)

--Marc

---

**✂ Re: Automated Bank RISKS (Osborn, [RISKS-9.46](#))**

Jon Mauney <mauney@cscadm.ncsu.edu>

Wed, 22 Nov 89 14:36:57 EST

In comp.risks osborn@cs.utexas.edu (John Howard Osborn) writes

>My bank, First Interstate, has recently implemented a handy new service.  
>... The problem is that the system also allows merchants  
>to check a check. That is, will a check, for a certain amount, from a certain  
>account, clear at this time? There is no security for this procedure.

Actually, this is another case of technology making things easier, but not making a fundamental change. I have an acquaintance who used to manage a small shopping center. He performed a simple search on a deadbeat tenant's account by calling the bank

"I have a check for \$1000. Is it good?"

then calling a different branch

"I have a check for \$2000. Is it good?"

etc. He was then able to tell the tenant exactly how much back rent would be paid that month. It is an amusing story when told from the point of view of my acquaintance, not so amusing from a privacy viewpoint.

Jon Mauney

---

**✂ Re: Autodialing horror stories (John, [RISKS-9.45](#))**

<Robert.Sansom@CS.CMU.EDU>

Tue, 21 Nov 89 09:19:35 -0500 (EST)

> ... A lady in Utah started getting anonymous phone calls in June, 1974.

The area code for Utah is 801.

> We investigated and discovered that there was a phone number that was  
> one dial pulse (there were lots of pulse-dial only exchanges then)  
> away from the 800 number that the computers were supposed to call.  
> We called the number and discovered on very frustrated lady! Ramada  
> [paid] for her to get a new phone number, and the problem went away.

The only area code that is one pulse away from 800 is 809. This is the  
area code for Bermuda, Puerto Rico, Virgin Islands and The Bahamas.

Did the lady in Utah have an 800 number? Or was she having her calls  
forwarded from her winter residence in St. Johns? 8-)

Robert Sansom, School of Computer Science, Carnegie Mellon University

[Or is the story apocryphal? 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 9: Issue 48

Saturday 25 November 1989

## Contents

- [Check inquiry / binary search](#)  
[anonymous](#)
- [Re: Training programmers](#)  
[Paul J. Mech](#)
- [Telephone Overload](#)  
[Jon von Zelowitz](#)
- [Write protect tabs](#)  
[via Peter Jones from Craig Finseth in VIRUS-L](#)
- [High error rates](#)  
[P.E.Smee](#)
- [Policy vs. the Enabling Technology](#)  
[Bill Murray](#)
- [Computer Virus Catalog Index: November' 89](#)  
[Klaus Brunnstein](#)
- [CERT\\_Tools\\_Announcement](#)  
[Edward DeHart](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✉ [Check inquiry / binary search \(Mauney, \[RISKS-9.47\]\(#\)\)](#)

<"anonymous">

Sat, 25 Nov 89 13:05:00 [x]ST

Jon Mauney's story about using check inquiries to determine the balance in an account rang a familiar bell. My mother once managed several apartment complexes. One month a deadbeat tenant gave her a \$250 check which bounced. When the check was returned, my mother used the same method described by Mauney to determine that the account had a balance of \$220. She then went to the bank, deposited \$30 cash in the deadbeat's account, and cashed the \$250 check. I've always wondered what the deadbeat's reaction was when he discovered what happened.



## Re: Training programmers (Ridgway, [RISKS-9.47](#))

<paul@oucsace.UUCP>  
25 Nov 89 05:36:08 GMT

A friend of mine, in part inspired by my success as a programmer, decided to enroll in a two quarter "Computer Programmer" course of study at a Columbus, OH, trade school. After a week, she had learned how to turn on an IBM PC clone without it exploding or chasing people around the room. By the end of the fourth week she had "learned Lotus." They then proceeded to the complexities of BASIC. In just a few short weeks, she "learned BASIC." She couldn't describe any but the simplest of algorithms and had no means of attack for simple programming problems, but she could tell me all the "command words" in the language. She dropped out before they got to the crowning achievement of the program, DBASE III.

All through this time I was incredulous. These people expected to be programmers. They were told that "starting salary for some programmers is \$35/hr." Yet they weren't even addressing fundamental algorithms, common approaches to problem solving, or anything more than a Jr. High level "Here is a word problem. Now solve it." I approached an instructor/administrator at the school with some of my reservations and was told that they were being taught "enough to get out into the workplace." What amazed me even more was that my knowledge of "real programming" far exceeded his, even though my schoolwork was in Physics, not CS.

No, I would not hire a graduate of such a program. Neither it seems would much of Columbus. We had subsequent contact with four of the graduates of the program. Only one had been employed in "computer programming" within four months of graduation. He had worked for a week on a problem that was entirely too advanced for him, and been allowed to resign gracefully. (Two were working as cashiers, the fourth unemployed.)

Paul J. Mech

---

### **☛ Telephone Overload**

Jon von Zelowitz <vonzelow@adobe.com>  
Fri, 24 Nov 89 15:19:21 PST

I discovered that MCI (my default long-distance company) was having a bad day when I tried to call my folks on Thanksgiving afternoon. I tried four times in a row, and each time, instead of being connected (or getting a "sorry" recording), I was patched into other peoples' conversations. What a failure mode!

After satisfying myself that MCI had a bug, I selected ATT (10288+number) and made my call. But most telephone users probably don't know how to do that (despite ATT's best efforts); in the US we have become accustomed to phones always working right.

(I am not an employee or stockholder of MCI or ATT. MCI usually works fine.)  
...sun!adobe!vonzelow vonzelow@adobe.com Jon von Zelowitz



David desJardins mentions a set of figures I've heard before, to wit

... look at neutron-activation bomb detectors, to be installed in airports. They are said to have something like a 3% false positive rate. ... Let's say that it [rate of bags with bombs to bags without] is 1 in 30 million ... That corresponds to 1 million false positives for every true positive. \*That\* is a high rate of error. And our society has chosen to spend nearly a billion dollars on that system.

I'd question whether a system with such a high rate of error will help, or whether it might not actually make things worse. If the operator knows (or works out from experience, as they certainly will even if they are not told) that out of every million bags which the system says need looked at by the bomb squad, only one actually contains anything suspicious, then it must be painfully tempting to say 'well, I'm in a hurry today, can probably let just this one through'. And of course since this will usually be 'right' in the sense that nothing untoward will happen, it will tend to be self-reinforcing carelessness. I can see where such a system might create a false sense of security based on 'gosh, new technology that can detect any form of explosive' while in fact increasing the chances of non-detection owing to the 'boy who cried wolf' syndrome.

In short, while more research is almost certainly worthwhile, I don't believe that putting this system into service in its present state of development could be considered a responsible act. Probably win votes, though.

Paul Smee | JANET: Smee@uk.ac.bristol  
Computer Centre | BITNET: Smee%uk.ac.bristol@ukacrl.bitnet  
University of Bristol | Internet: Smee%uk.ac.bristol@nsfnet-relay.ac.uk  
(Phone: +44 272 303132) | UUCP: ...!uunet!ukc!gdr.bath.ac.uk!exspes

---

### **✂ Policy vs. the Enabling Technology (Randall Davis, [RISKS-9.45](#))**

<WHMurray.Catwalk@DOCKMASTER.NCSC.MIL>

Mon, 20 Nov 89 22:32 EST

>Right, and then we should discuss the POLICY, not the technology  
>that made it worth discussing. [...]

Most of us seem to understand this intuitively; nonetheless, we consent to have the debate on the technology, rather than the policy. We continue this not at our peril, but at the risk of an orderly society.

William Hugh Murray, Fellow, Information System Security, Ernst & Young  
2000 National City Center Cleveland, Ohio 44114  
21 Locust Avenue, Suite 2D, New Canaan, Connecticut 06840

---

### **✂ Computer Virus Catalog Index: November '89**

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

21 Nov 89 17:37 GMT+0100

The Computer Virus Catalog now classifies 45 viruses (AMIGA:24;MSDOS:15; Atari:6). Activities are undertaken to make the documents available via servers in different regions of the world; we hope that we can announce such servers in the next weeks. If you wish to receive the documents (see Index appended, with length of the documents given) sooner, please send a short request to the author.

Klaus Brunnstein

```

=====
==          Computer Virus Catalog Index          ==
=====
==  Status:   November 15, 1989 (Format 1.2)      ==
==  Classified: 15 MSDOS-Viruses (MSDOSVIR.A89)    ==
==             24 AMIGA-Viruses (AMIGAVIR.A89)    ==
==             6 Atari-Viruses (ATARIVIR.A89)     ==
== Updates   since last edition (July 31, 1989) marked: U (column 70)=U=
== Additions since last edition (July 31, 1989) marked: + (column 70)=+=
=====
== Document MSDOSVIR.A89 contains the classifications of the ==
== following viruses (1.138 Lines, 6.271 Words, 62 kBytes): ==
==                                                     ==
== 1) Autumn Leaves=Herbst="1704"=Cascade A Virus      ==
== 2) "1701" = Cascade B = Autumn Leaves B = Herbst B Virus ==
== 3) Bouncing Ball = Italian = Ping Pong= Turin Virus  =U=
== 4) "Friday 13th" = South African Virus              =+=
== 5) GhostBalls Virus                                =+=
== 6) Icelandic#1 = Disk Crunching = One-in-Ten Virus  =U=
== 7) Icelandic#2 Virus                               =+=
== 8) Israeli = Jerusalem A Virus                      =U=
== 9) MachoSoft Virus                                  =+=
== 10) Merritt = Alameda A = Yale Virus                ==
== 11) Oropax = Music Virus                            ==
== 12) Saratoga Virus                                  =+=
== 13) SHOE-B v9.0 Virus                               ==
== 14) VACSINA Virus                                   =+=
== 15) Vienna = Austrian = "648" Virus                 =U=
==                                                     ==
== Remark: The following 13 MS-DOS-Viruses are presently being classi==
== fied and will be published in the next edition (December 31,1989): ==
== .) Brain A = Pakistani A-Virus      (Pakistani Virus Strain) ==
== .) Datacrime I = 1168 Virus          (Datacrime Virus Strain) ==
== .) Datacrime II = 1280 Virus         (Datacrime Virus Strain) ==
== .) Den Zuk Virus                    (Venezuela/Search Virus Strain) ==
== .) Lehigh Virus                      ==
== .) FuManchu Virus                    (Israeli Virus Strain) ==
== .) NewZeeland= Marijuana= Stoned Virus (NewZealand Virus Strain) ==
== .) Pentagon Virus                    ==
== .) SURIV 1.01,2.01,3.00 Viruses     (Israeli Virus Strain) ==
== .) Traceback Virus                  ==
== .) 405 Virus                        ==
=====
== Document AMIGAVIR.A89 contains the classifications of the ==

```

== following 24 viruses (2.272 Lines, 9.421 Words, 106 kBytes): ==

- ==
- ==
- == 1) AEK-Virus = Micro-Master Virus (SCA Virus Strain) =U=
- == 2) BGS 9-Virus =+=
- == 3) Byte Bandit Virus =U=
- == 4) Byte Bandit Plus Virus (Byte Bandit Virus Strain) =+=
- == 5) Byte Warrior#1 Virus = DASA-Virus (Byte Warrior Strain) =U=
- == 6) Disk Doctors Virus =U=
- == 7) Gaddafi-Virus =U=
- == 8) Gyros Virus =U=
- == 9) IRQ-Virus =U=
- == 10) LAMER (Exterminator) Virus =U=
- == 11) LSD Virus (SCA Virus Strain) =+=
- == 12) NORTH STAR I Antivirus-Virus (NORTH STAR Virus Strain) =U=
- == 13) NORTH STAR II Antivirus-Virus (NORTH STAR Virus Strain) =U=
- == 14) Obelisk Virus =U=
- == 15) Paramount Virus = Byte Warrior#2 Virus (Byte Warrior Strain) =U=
- == 16) Pentagon Antivirus-Virus =+=
- == 17) Revenge 1.2G Virus =+=
- == 18) SCA-Virus =U=
- == 19) System Z 3.0 Antivirus-Virus (System Z Virus Strain) =U=
- == 20) System Z 4.0 Antivirus-Virus (System Z Virus Strain) =U=
- == 21) System Z 5.0 Antivirus-Virus (System Z Virus Strain) =+=
- == 22) Timebomb 1.0 Virus =+=
- == 23) VKill 1.0 Virus = Camouflage Virus =U=
- == 24) WAFT-Virus =+=

== Remark: the following 8 AMIGA-viruses are presently analysed, clas=  
 == sified and will be published in the next edition (12/31/1989): ==

- == .) BUTONIC 1.1 Virus ==
- == .) JOSHUA Virus ==
- == .) LAMER EXTERMINATOR Virus 1.0, 2.0, 3.0 ==
- == .) SYSTEM Z 5.1, 5.3 Virus ==
- == .) WARHAWK Virus ==

=====  
 == Document ATARIVIR.A89 contains the classifications of the ==  
 == following 6 viruses (375 Lines, 2.045 Words, 21 kBytes): ==

- ==
- ==
- == 1) ANTHRAX = Milzbrand Virus =+=
- == 2) c't Virus ==
- == 3) Emil 1A Virus = "Virus 1A" ==
- == 4) Emil 2A Virus = "Virus 2A" = mad Virus ==
- == 5) Mouse (Inverter) Virus =U=
- == 6) Zimmermann-Virus ==

== Since last edition, ANTHRAX V. has been added. We have problems to ==  
 == get viruses, as many users wish to exchange their viruses (like ==  
 == stamps) against our's, which we generally refuse: the Virus Test ==  
 == Center's ethical standard says, that we do not spread viruses! ==  
 == Please send infected programs without preconditions. ==

=====  
 == For essential updates (marked "U="), we wish to thank D.Ferbrache,==  
 == Y.Radai and F.Skulason for their continued help and support. ==  
 == Critical and constructive comments as well as additions are ==

```
== appreciated. Especially, descriptions of recently detected viruses =
== will be of general interest. To receive the Virus Catalog Format, ==
== containing entry descriptions, please contact the above address. ==
=====
=====
== The Computer Virus Catalog may be copied free of charges provided ==
== that the source is properly mentioned at any time and location ==
== of reference. ==
=====
== Editor: Virus Test Center, Faculty for Informatics ==
== University of Hamburg ==
== Schlueterstr. 70, D2000 Hamburg 13, FR Germany ==
== Prof. Dr. Klaus Brunnstein, Simone Fischer-Huebner ==
== Tel: (040) 4123-4158 (KB), -4715 (SFH), -4162(Secr.) ==
== Email (EAN/BITNET): Brunnstein@RZ.Informatik.Uni-Hamburg.dbp.de ==
=====
== This document: 117 Lines, 701 Words, 9 kBytes ==
=====
```

---

## **CERT\_Tools\_Announcement**

*Edward DeHart <ecd@cert.sei.cmu.edu>  
Fri, 17 Nov 89 23:10:52 EST*

The Computer Emergency Response Team Coordination Center (CERT/CC) has established a new Internet mailing list named CERT-TOOLS.

The purpose of this new mailing list is to encourage the exchange of information on security tools and security techniques. The list should not be used for security problem reports.

The CERT/CC has found that many sites have developed tools and techniques to improve the security of their systems (e.g. tools to assist users' selection of passwords that are difficult to guess, account management techniques, monitors that help detect unauthorized system access). Also, several tool developers have expressed an interest in sharing their work with others. We hope this mailing list will spawn new security tool development and allow individual sites to take advantage of existing work.

The mailing list will not be moderated and the CERT/CC will not formally review, evaluate, or endorse the tools and techniques described. The decision to use the tools and techniques described is the responsibility of each user or organization and we encourage each organization to thoroughly evaluate new tools and techniques before installation or use.

Membership is restricted to system programmers, system administrators and others with a legitimate interest in the development of computer security tools. If you would like to be considered for inclusion, please send mail to:

cert-tools-request@cert.sei.cmu.edu

You will receive confirmation mail when you have been placed on the list.

We ask that the mailing list not be used for file transfers. If you have a tool or technique that you would like to share, please mail a description of the tool or technique to the mailing list and describe how others can acquire the tool or obtain additional information. The CERT/CC is planning to collect many of the tools and will make the archive available via anonymous ftp on the cert.sei.cmu.edu system.

All mail intended to be redistributed should be mailed to:  
cert-tools@cert.sei.cmu.edu

Please feel free to inform other colleagues interested in security tools and security techniques about this list. Also, please send comments, criticisms, and suggestions on this or any other CERT/CC activity to:  
cert@cert.sei.cmu.edu

Thank you,  
Ed DeHart, Computer Emergency Response Team  
Email: cert@cert.sei.cmu.edu  
Telephone: 412-268-7090 (answers 24 hours a day)

-----

Affiliation: \_\_\_\_\_  
Name (last, first, MI): \_\_\_\_\_  
Title: \_\_\_\_\_

Address: \_\_\_\_\_ Phone Numbers:  
\_\_\_\_\_ Work: \_\_\_/\_\_\_\_\_  
\_\_\_\_\_ Home: \_\_\_/\_\_\_\_\_  
FAX: \_\_\_/\_\_\_\_\_

City: \_\_\_\_\_ Pager: \_\_\_/\_\_\_\_\_  
State: \_\_ Zip: \_\_\_\_-\_\_\_\_ Computer Room:  
Country: \_\_\_\_\_ /\_\_\_\_\_

Email Address: \_\_\_\_\_

Supervisor's Name: \_\_\_\_\_ Phone Number: \_\_\_\_\_

Return form via email to cert-tools-request@cert.sei.cmu.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 9: Issue 49

Monday 27 November 1989

## Contents

- [Davis on arguing about technology vs policy](#)  
[Phil Agre](#)
- [Re: Check inquiry / binary search: Gardner](#)  
[Jim Griffith](#)
- [Re: Check inquiry / binary search: Theroux](#)  
[Roy Smith](#)
- [Re: Privacy and risks in credit information](#)  
[Brinton Cooper](#)
- [Re: UNIX EXPO Blackout"](#)  
[Glenn Story](#)
- [How to improve your financial standing](#)  
[Glenn Story](#)
- [Re: Self-trust and computer professionals](#)  
[Mike McNally](#)
- [Re: problems with government project specifications](#)  
[Bob Estell](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✉ [Davis on arguing about technology vs policy](#)

"Phil Agre" <[agre@gargoyle.uchicago.edu](mailto:agre@gargoyle.uchicago.edu)>  
Sat, 25 Nov 89 15:40:52 198

Randy Davis certainly offers a coherent argument and we should be clear just how much it would take to refute it. His argument, at least as I understand it, requires that one accept no more than our society's usual definition of engineering as an instrumental activity: ends are to be distinguished from means; society decides upon its ends; and engineering concerns itself with the means. If new technology facilitates certain forms of invasion of privacy, then that calls for a societal decision about privacy, not about technology. To refute this argument (if that is something one wishes to do) one must address this distinction between ends and means, arguing either that it does not make sense, that it does not and could not remotely approximate the actual conditions, or that it is inherently unhealthy for us to organize our thinking

in those terms. All of these arguments have been made [\*], though not so far as I recall on the Risks list. Arguing the points in the abstract would presumably be a uselessly redundant activity, but using the many examples that come up on the list to explore them concretely could well be constructive.

Phil Agre, Computer Science Department, University of Chicago

[\*] Some of the standard references are:

Hannah Arendt, "The Human Condition"

Martin Heidegger, "The Question Concerning Technology"

Theodor Adorno and Max Horkheimer, "Dialectic of Enlightenment"

Stanley Aronowitz, "Science as Power"

Jurgen Habermas, "Science and Technology"

Bruno Latour, "Science in Action"

Carolyn Merchant, "The Death of Nature"

---

**✉ Re: Check inquiry / binary search: Gardner (Mauney, [RISKS-9.47](#))**

*Jim "The Big Dweeb" Griffith <griffith@scam.Berkeley.EDU>*

*Sat, 25 Nov 89 16:29:23 -0800*

This scenario was used in *\_THE CASE OF THE BEAUTIFUL BEGGAR\_*, a Perry Mason mystery by Erle Stanley Gardner. In it, a wealthy elderly man was institutionalized by his money-grubbing relatives, and they got a court order that forced the bank to turn over all of the man's assets. Well, the man had previously written a \$125,000 check to a niece of his (who wasn't money-grubbing, just poor). But there was no money in the account to cover it, because of the court order. After the court order, the bank received a \$50,000 deposit for that man's account from a past-due business transaction. Mason took out a loan for \$75,000, deposited it in the account, cashed the \$125,000 check, and repaid the loan, along with \$12.50 interest, all within 15 minutes. And it was entirely legal, because the court order had specified that the bank had to turn over all money \*currently\* deposited in the bank. The book mentioned here was published in 1965.

Jim

---

**✉ Re: Check inquiry / binary search: Theroux (Mauney, [RISKS-9.47](#))**

*Roy Smith <roy@alanine.phri.nyu.edu>*

*Sun, 26 Nov 89 09:07:54 EST*

As with the case of the library card records recently discussed, there is nothing particularly new about this risk just because computers have made it easier to exploit. In chapter 7 of Paul Theroux's novel "Fong and the Indians", published in 1968, exactly the same scheme is used to cash at least part of a meant-to-bounce 1000 shilling check against a 632 shillings ninepence balance. The book does not make it clear how the actual balance in the account was discovered, however.

Roy Smith, Public Health Research Institute, 455 First Avenue, New York, NY 10016

---

**✂ Re: Privacy and risks in credit information (Gorman, [RISKS-9.46](#))**

Brinton Cooper <abc@BRL.MIL>  
Sun, 26 Nov 89 16:42:27 EST

John DeBert, in the referenced article provides a good summary of TWR's "promised practice" in protecting the privacy of credit records while affording anyone access to his/her own information.

It's chilling to reflect upon the fact that, in my community, TRW runs a for-profit alcoholism treatment center to which first-time DWI offenders are often sent for treatment as part of a program of "probation before judgement." One wonders how mutually compartmented these TRW operations are?

\_Brint

---

**✂ re: UNIX EXPO Blackout"**

<story\_glenn@comm.tandem.com>  
27 Nov 89 14:35:00 -0800

I forwarded Brian Randell's item, "UNIX EXPO Blackout" from RISKS forum 9.45, to Tandem's internal mail system. I received several responses which seemed to fall into one of two categories: (1) requests for more information, and (2) justifications of Tandem's performance in the "race" described in the article.

I found these responses curious since they seemed to disregard the fact that I was merely repeating third- or fourth-hand information.

Meanwhile, no one seems to have noticed this fatal flaw in the original contest: fault tolerance has no direct relationship with how fast a computer restarts after a power failure (unless, of course, it fails to come up at all). Even computers that make no claims whatever about fault tolerance (such as the lowliest PC) still are expected to restart after a power outage.

Glenn Story, Tandem Computers, story\_glenn@comm.tandem.com

---

**✂ How to improve your financial standing**

<story\_glenn@comm.tandem.com>  
27 Nov 89 16:28:00 +1600

A recent RISKS posting on credit information reminded me of an incident that happened to me a few years ago.

Due to some flaw in my personality, I love to fill out questionnaires. One day I received a "marketing" questionnaire on oil-well speculations, the last question of which was "Would you be interested in hearing about opportunities in this area?" I answered that one, "no" and mailed the questionnaire off.

Soon I started receiving phone calls from oil-well salesmen. Having forgotten all about the questionnaire, I asked one of these salesmen where he got my name. He said from some data service in Texas; he even read my profile which described me as a "wealthy entrepreneur who likes to invest in high-risk projects".

I wrote to the company sending the data, informing them of their error. They responded with a form letter explaining my rights under the Fair Credit Practices Act. Since their information about me was not derogatory, I did not respond.

Later when I got yet another sales call I explained about the flakey data base in Texas. The salesman responded that he didn't get my name from there--he got it from Dunn and Bradstreet!

So, now that I'm rich, I'm working on famous. Anyone know who runs the computers for "Who's Who in America"?

Glenn Story, Tandem Computers, story\_glenn@comm.tandem.com

---

### **✶ Re: Self-trust and computer professionals (Fagan, [RISKS-9.45](#))**

*Mike McNally <m5@lynx.UUCP>  
Mon, 27 Nov 89 09:31:10 PST*

The other day, whilst merrily shopping at my lovely neighborhood Mervyn's, I overheard a conversation between a gentleman buying some clothes (shirts I think) and the cashier. A disagreement arose over the price of a shirt: the customer thought it was on sale for 14.95, but the "computer" responded to the bar code with a price of 15.99. (Note: all the price tags I saw had the price clearly printed, by "the computer" of course, beneath the bar code. Perhaps the tag in question had been mutilated.) The customer, not at all irate, wanted to check the price he thought was advertised on a small placard above the display on which he found the garment. The salesperson gladly agreed, but pointed out two things: first, that they never have prices that are NN.95; second, that "the computer is usually right". The customer grinned and said "No, I build systems, and I know that's not true."

"Well, gee," I thought to myself. I work on computer systems, and while I know that they have the potential of being pretty danged wrong in pretty big ways, I also know that the salesperson was right: *usually* the computer is right; or, more precisely in this case, when she presents the UPC code to the POS terminal, and the thing likes it and responds with the price that matches the code, most of the time it will be correct. It may be the case that the database has not been properly updated to match short-term sales, as (apparently, from previous postings in RISKS) happens in grocery stores, but I really must wonder if it's correct to say that the computer is "wrong". In the Mervyn's example, there is the additional "ECC" of the Mervyn's pricing scheme, which only allows certain fractions. (In the end, the customer decided that the computer was right after all.)

I'm as leary of computerization as the next man, but not to the point of having an almost manic distrust. I'm not an auto mechanic or designer, but off the top of my head I can name a few critical systems that could fail on 280 at 70 mph with disastrous consequences. I still drive. I ride a bicycle, but I can't really say I trust those little spokes. In short, I don't have complete faith in *\*any\** system I trust with my life, but I use (and rely on) those systems nevertheless.

Mike McNally Lynx Real-Time Systems 408 370 2233

---

## ✂ RE: problems with government project specifications

"FIDLER::ESTELL" <estell%fidler.decnet@nwc.navy.mil>

27 Nov 89 14:13:00 PDT

Like almost all old [more than 70 years], large [more than 10,000 people] institutions, the government did not get to be as successful as it is by acting the way it does now. [Paraphrased from the original statement by Robert Townsend, in *\_Up the Organization\_*. He was talking about GM. Similar symptoms, probably same causes.]

An all too typical scenario for developing the technical section of a DoD RFP [request for proposal] is that some technical folks may write 10 pages of plain English, describing what they want; e.g., a typical mini-computer RFP may begin with a list of software tools and applications that the users must have; then talk about reliability, so that the uses will indeed be able to work; then mention cost, so that bidders don't blow the budget; then specify that the new system must interface to the extant network; and finally, within those constraints, be as fast as possible.

Enter then the good people who must actually negotiate the contract. Usually, that means least cost, or best bargain. So the above RFP gets rewritten to put cost first, and speed next; the software gets put in as a list of "mandatory" and/or "desirable" options. [Yes, that's one of my favorite oxymorons - "mandatory option."] Reliability is addressed in terms of guaranteed response times to failures. [An argument was once made by H-P that it is better to respond in two days to only one failure per year, than in two hours to a failure every week. Sometimes the government accepts such logic; sometimes not.] Network interface is often left as an exercise for the buyer. [On other occasions, "compatibility" becomes the reason for a sole source buy of a the same brand, similar model.] In most cases, those 10 pages now number over 100. And the rewrite usually takes 6 months or more.

At the extreme, we have written specifications for systems that the vendors do not make; e.g., instead of saying that we want lots of disk capacity in little floor space, we specify drive characteristics. That has led to some "no bid" responses, much to the consternation of both sides. And the process then exceeds a year, including rewrites. In that much time, the project needs have evolved, since 25% to 35% of the project schedule has elapsed; and of course the computer industry has evolved too; almost one PC-generation has passed.

Ancient wisdom tells us that "Too many cooks spoil the broth." That "A camel is a horse designed by a committee." Modern wisdom [Robert Heinlein] tells us

that "A committee is an animal with at least 6 legs and no brain."

Why do we do this? One good friend, Harry Parode, says that we only strive to spend public funds honestly. Somehow, we seem to feel that, if enough people contribute enough words, the RPF, and the resulting system, will be better. I doubt it. I tend to agree with the lesson in the story told after CRAY Research built a better scientific computer than mighty IBM: Thomas Watson asked how three dozen folks could beat a team of about 1000; when Seymour Cray was told of the inquiry, he opined, "I believe Mr. Watson has answered his own question."

Bob

Disclaimer: The opinions herein are my own; and I know darn well that the government does NOT agree.



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 9: Issue 50

Sunday 3 December 1989

## Contents

- [Vote counting problems - experience in Michigan](#)  
[Lawrence Kestenbaum](#)  
[PGN](#)
- [Specs and custom software](#)  
[Curtis Jackson](#)
- [Pentagon Computer Costs](#)  
[Gary Chapman](#)
- [Software tool munges code](#)  
[Nick Lai](#)
- [Marshall Williams convicted of destroying data](#)  
[PGN](#)
- [Mitnick's accomplice sentenced](#)  
[Rodney Hoffman](#)
- [Desktop forgery](#)  
[Rodney Hoffman](#)
- [Paul Brodeur's "Currents of Death"](#)  
[Werner Uhrig](#)
- [McRisks - Electronic Interference in Fast Food Automation](#)  
[Robert Horvitz](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✉ Vote counting problems - experience in Michigan

<WCLX@VAX5.CIT.CORNELL.EDU>

Wed, 29 Nov 89 20:38 EDT

I have followed with interest the recent discussions of vote-counting errors in Durham NC, Yonkers NY and elsewhere. Perhaps the following may be of interest. It is a discussion of a specific vote counting problem in a jurisdiction where I served until last year as an elected official.

Lawrence Kestenbaum, 506 S. Albany St., Ithaca NY 14850 (607) 272-7750

[grad student at Cornell University in City and Regional Planning

(specializing in Historic Preservation), an attorney licensed in Michigan (number P34957), and a former Ingham County Mich Commissioner, elected from the 8th District in 1982, 1984 and 1986. Nothing in this message is private or privileged information.]

-----

Some of the recent problems with inaccurate election-night vote tallies can be traced to the badly-handled interface between computer and manual systems. Non-electronic vote counts, for example, are mistyped on computer screens during the hectic atmosphere of election night. Of course, when the computer system plays the dominant role, the difficulties with the non-computerized parts are even greater.

While most of the Northeast still votes on the old-style lever machines, the Midwest -- Michigan at least -- has largely moved to computer punch card ballots. Punch cards have certain advantages: in the event of a recount, a tangible, anonymous record exists of each voter's choices. By contrast, recount lawyers are often able to find whole voting machines whose votes must be excluded from the count because of mechanical problems, thus disfranchising anyone who voted on that machine. Other problems are possible, but all in all, results from punch card jurisdictions are regarded as being much more 'firm' and resistant to being altered in recounts and challenges. At the same time, it lulls political people into a sometimes unjustified faith in computer-generated vote tallies.

When I served on the county board in Ingham County, Michigan (1983-88), we had a mixed system. The choice of voting method was made individually by the 21 townships and cities within the county. Thanks to strong persuasion by the county clerk, almost all of the 250 or so voting precincts in the county voted on punch cards. The remaining five precincts, in four small jurisdictions, used voting machines; absentee voters in those five precincts used punch cards. In no other part of the county were absentee votes counted separately. Under contract with most of the punch-card jurisdictions, the county provided the materials and organized the ballot counting process.

The software which aggregated and reported the votes for the county, and also automatically generated all of the official statements to be attested to by the Board of Canvassers, did not allow for the entry of non-computer precincts. Thus, the county clerk's people had to break into the program and override its security features in order to input the numbers for the five rogue precincts. The risks here should be obvious! Invariably, this task was postponed until very late at night, when the operators (who normally worked 8am to 5pm) were extremely tired. More than once, as I recall, this led to errors in the overall totals, though none which changed the outcome, and all were corrected by the following day.

After a few years of this, the county clerk (with full support from the county board) mounted a major effort to corral the five remaining precincts. He succeeded with all but one of them, the City of Leslie. So, on a smaller scale, the problem -- and RISK -- continues.

Lawrence Kestenbaum, wclx@vax5.cit.cornell.edu

---

## ✂ Vote counting problems - experience in Michigan (Kestenbaum)

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

Sun, 3 Dec 1989 12:57:33 PST

Lawrence Kestenbaum's message gives an interesting first-hand account. However, there is much debate in the election computing community about the relative tamperabilities of machine-readable cards (punched or mark-sensed), lever machines, and direct-entry screen menus. Punched cards give results that are more or less repeatable (ignoring the hanging chad problems). But they are subject to tampering BEFORE any votes are ever tabulated (removed cards, added cards, multipunched cards, hidden prepunches, trick punches that unleash Trojan horses, etc.), which can make the repeatability argument moot. The RECOUNT would mask the prior fraud and even add apparent credibility! The fantasy that there is a CORRECT anonymous physical record is very tricky to convert into a reality. (There are different vulnerabilities in the other types of systems, such as the presence of perfectly repeatable but hidden and probably undetectable Trojan horses in the direct-entry systems -- especially in proprietary systems. See earlier RISKS...)

---

## ✂ Specs and custom software (Re: [RISKS-9.47](#))

Curtis Jackson <jackson@adobe.UUCP>

30 Nov 89 23:13:32 GMT

I worked on custom military design for almost 7 years recently.  
I have two anecdotes to relate regarding recent RISKS discussions:

- 1) Some colleagues and I endeavored to design the operating systems for the latest in a series of custom large-control-word multi-processor signal processors using a purely waterfall model. We insisted on writing the design spec before writing any code, and finalizing the design spec (after initial review) down to the individual bit level. We then wrote pseudo-code for all modules, and peer-inspected those. Finally we wrote the code with strict commenting standards and assembled it, then peer-inspected that. Finally we wrote module tests, simulated those, then string tests, simulated those, and one day the hardware was off the drawing boards and in the lab. The results? The development cycle, with full waterfall design method and full regression tested test database, was only 2 months over schedule (former efforts on similar jobs ran up to a year over). The norm for getting a basic operating system up and running in a lab environment without bells and whistles was 6-9 months -- it took us a week. Overall savings in development/debug time -- probably at least 40%. Overall savings in down-the-road software maintenance -- untold. So let me say that I am skeptical at best when someone tells me that waterfall design should be dumped on large involved custom software/hardware projects.
- 2) I had a chance to have a several-hour chat with a Navy commander who headed the technical management on the Navy end of our several-hundred-million-dollar project. He noted that the average time for delivery of a large military contract now was 8 years and growing, and that the results were far from

satisfactory, particularly in the RISKS area. He blamed much of this on government procurement and the rampant cover-your-ass overspec'ing that went on. He proposed a system wherein the contractor(s) would study and prototype for some time, a year for example, then come back and note the 10% of the job that they felt was overspec and would cause serious money, time, and risk problems. Independent government negotiators would then attempt to take these portions out of the contract if they were indeed overspec, but the contractor would suffer little or no degradation in the original price quoted for the contract for their having pointed these overspecs out. He estimated the average deliverable time would go down to about 5 years, and the products delivered would be slightly cheaper and much more reliable. He also was sure his ideas would never fly at the Pentagon. :-(

Curtis Jackson @ Adobe Systems in Mountain View, CA (415-962-4905)  
uucp: ...!{apple|decwrl|sun}!adobe!jackson

---

### **✂ Pentagon Computer Costs**

*Gary Chapman <chapman@csl.stanford.edu>  
Fri, 1 Dec 89 11:22:11 PST*

The New York Times today (12/1/89) features a story by Jeff Gerth that says that the modernization of a Pentagon computer system used for general data processing is a billion dollars over budget, and far behind schedule. And the congressional report released about this system says that Pentagon computer systems have experienced "runaway costs and years of schedule delays while providing little capability."

Charles A. Bowsher, the head of the General Accounting Office, says that problems with the Pentagon's accounting system may impede efforts to reduce spending in the Department of Defense because of inaccuracies in the data used to manage the Department.

Today's New York Times article reports only on cost overruns and delays in accounting and data-processing systems used by the Department of Defense and the services. But there are also these examples one could add to the list:

- \* The C-17 cargo plane being built by Douglas Aircraft has a \$500 million cost overrun because of problems in its avionics software, and the software contractor has been fired, according to a member of Congress.
- \* The B-1 bomber still needs more than \$1 billion to improve its ineffective air defense software. The B-1 was originally sold as a "penetrating bomber," meaning it was supposed to be able to penetrate Soviet air defenses. Because of problems with its computer software, however, the B-1 is not expected to be able to penetrate Soviet air space, and that's why the Air Force is asking for the B-2 (which has its own software problems). (At one point the B-1 electronic countermeasures software created what

was called a "beacon" effect, meaning it would actually alert Soviet air defenses and give their radars a clearer signal of the aircraft than they would have if the airplane's systems had been turned off.)

- \* The software for the modernization of the Satellite Tracking Control Facility is about seven years behind schedule, about \$300 million over budget, and will provide less capability than what the original contract called for.
- \* The modernization of the software at NORAD headquarters is about \$250 million over budget, years late, and still non-operational.
- \* The Airborne Self-Protection Jammer (ASJP), which is an electronic air defense system installed in over 2,000 Navy fighters and attack planes, is \$1 billion over budget, four years behind schedule, and, according to a Navy report, is only "marginally operationally effective and marginally operationally suitable."

As General Bernard Randolph, commander of the Air Force Systems Command, said in February, "We have perfect record on software schedules--we have never made one yet and we are always making excuses."

Gary Chapman, Executive Director, CPSR

chapman@csl.stanford.edu

---

### **✂ Software tool munges code**

*Nick Lai <lai@east.Berkeley.EDU>*

*Thu, 30 Nov 89 15:53:24 PST*

The "indent" program (C code formatter) distributed with Berkeley UNIX has an insidious misfeature/bug in it. The bug is also present in the version that comes with SunOS. The Ultrix folks appear to have written their own "indent", which does not have the bug.

The problem is that "indent" takes expressions of the form "<ident>=-

---

### **✂ Marshall Williams convicted of destroying data**

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

*Fri, 1 Dec 1989 16:01:26 PST*

Marshall Williams, a former company cost estimator for Southeastern Color Lithographers Inc., Athens GA, was convicted on 16 Nov 89 for "using his company's computer network to destroy billing and accounting data as well as backup copies of that data". A key piece of evidence was a computer audit trail of data-deletion commands that traced deletions to his terminal. The defense raised the potential for a frame-up resulting from someone tampering with the audit trail data. (No one seems to have suggested that someone else

might have been using his terminal.)

The crime allegedly cost Williams' former employer more than \$400,000 in lost business and downtime. He faces up to 15 years in prison. Williams contended that he "knew nothing about his employer's complicated Xenix operating system and could not have deleted the data." He plans to appeal.

[Source: PC Week, 27 November 1989, p.1, article by Richard March]

---

### ✦ **Mitnick's accomplice sentenced**

*Rodney Hoffman <Hoffman.ElSegundo@Xerox.com>*

*1 Dec 89 14:39:33 PST (Friday)*

Leonard DiCicco was once a friend of convicted hacker Kevin Mitnick (see RISKS 9.6 and 9.7). In July, DiCicco pleaded guilty to charges of permitting Mitnick to gain access to a computer at DiCicco's workplace last December, which was then used to steal a \$1-million DEC security software program.

According to a small notice in the "Los Angeles Times" 30-Nov-89, DiCicco has now been sentenced to 5 years' probation, plus 750 hours of community service, part of which will be spent installing a computer system at a shelter for the homeless.

---

### ✦ **Desktop forgery**

*Rodney Hoffman <Hoffman.ElSegundo@Xerox.com>*

*1 Dec 89 17:59:20 PST (Friday)*

DESKTOP FORGERY, by David Churbuck, is the cover story in the 27-Nov-89 issue of "Forbes". It tells how to scan in a check, alter it, print it, and pass it (with a few details omitted), and it tries to frighten bankers and others with the endless possibilities.

Churbuck does note, "To be sure, the desktop computer did not create the crime of forgery. All it did was make the tools user-friendly. Check-passers can now practice forgery in the privacy of their own homes...."

---

### ✦ **Paul Brodeur's "Currents of Death" (new book)**

*Werner Uhrig <werner@rascal.ics.UTEXAS.EDU>*

*Thu, 30 Nov 1989 3:16:45 CST*

On the CBS program NightWatch (for vampires and am-hackers) I just watched an interview with Paul Brodeur who wrote those articles in the New Yorker this spring on the danger of radiation of electrical fields (high voltage power-lines, heating blankets, display terminals) and who has just come out with a new book titled "Currents of Death" which some of you may want to put on your Xmas reading list also.

I had not realized this before, but this man was also in the forefront of the battle of getting the public's attention on the Ozone problem (10 years ago) and the Asbestos problem (20? years ago). A man worth paying attention to, it seems.

---

## ✂ McRisks - Electronic Interference in Fast Food Automation

Robert Horvitz <rh@well.UUCP>

Sat, 4 Nov 89 22:33:34 pst

"The Importance of EMC in the Preparation and Selling of Big Macs," by Fernando M. Esparza is a fascinating article in the September- October 1989 issue of "EMC Technology." (EMC = Electromagnetic Compatibility, the science/art of getting electronic devices to work properly without interfering with one another.)

Esparza, the author of McDonalds' "Electrical Disturbance Standards," has some great war-stories to tell about problems cropping up in these highly automated fast-food environments due to unforeseen interactions among appliances. One he described as "the most serious interference incident that McDonalds has ever experienced" involved toasters and timekeeping.

It seems that when McDonalds decided to introduce McMuffin products, they had to install special toasters. Soon, many of their employee time-clocks inexplicably started to gain 2 to 4 hours each day, crediting workers with more hours than they had actually worked. After a lot of head-scratching (and testing), they discovered that the new toasters' voltage control circuits induced voltage spikes in the powerline during normal operation - sometimes as many as 120 per second. This disrupted the clocks on the same power circuit, since they monitored the alternating current's waveform for the purpose of time-keeping: the voltage spikes increased the number of "zero-crossings," which were used as the metric.

"By the time we were able to pin down the problem exactly, there were more than 5,000 toasters installed in the restaurants... Some restaurants reverted to manual procedures for payroll timekeeping, but there were a number of employees who were paid for extra time because of the clock errors. Although the managers were understandably upset, none of the crew complained."

"Ghosts in the Drive-Thru" was another baffling problem, affecting the POS (point-of-sale) system of a McDonalds in suburban Los Angeles: "The POS system is a collection of computerized cash registers that are networked together in a somewhat sophisticated and proprietary network," Esparza explains. The problem was that bogus food orders showed up randomly in the system. "The restaurant could distinguish ghost orders from real orders because the quantity of the items displayed was the same - 11 cokes, 11 fries, 11 hamburgers, etc. The items themselves were directly copied from the previous, actual order. These orders could not be cancelled but had to be cashiered out of the system, thereby rendering all product mix and sales information invalid and creating a potential security/theft problem, in addition to slowing customer service in the drive-thru."

The restaurant's POS system and all of its software was replaced, but the problem continued. To make a long story short, this McDonalds happened to be near a cluster of radio and television transmission towers. The POS system's wiring acted as an antenna, capturing the signals, and corrupting some of the data that flowed thru the wires.

One problem described in this article stands out as a potential threat to many more retailers than just McDonalds: "The Cash Drawers that Opened by Themselves." Again making a long story short, Esparza discovered that the problem began soon after the local police department upgraded their communications system with higher-power mobile radios. "Whenever they responded to a call while in the drive-thru, the cash drawers opened... An open cash drawer without a cashier to supervise it is...a large security liability."

Have any RISKS readers heard of police radio transmissions inadvertently opening other businesses' cash registers?

["EMC Technology" is a controlled circulation bimonthly. Subscriptions are free to those who qualify, \$40/year for those who don't. For more information contact EMC Technology Circulation Dept., 5615 West Cermack Rd., Cicero, IL 60650-2290 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 9: Issue 51**

**Tuesday 5 December 1989**

## Contents

- [Computer bungling of auto insurance premiums](#)  
[Barry Kolb](#)
- [Computerized voting machine misbehaves](#)  
[Rodney Hoffman](#)
- [Re: Vote counting problems - experience in Michigan](#)  
[Jeffrey R Kell](#)
- [Privacy issues raised about automating toll collection](#)  
[Stephen W Thompson](#)
- [Re: Electronic Interference in Fast Food Automation](#)  
[David Chase](#)
- [Digital Cellular and the government](#)  
[Tim Russell](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✂ Computer bungling of auto insurance premiums

*Barry Kolb <70426.1251@CompuServe.COM>  
03 Dec 89 22:41:42 EST*

PGN's calling for RISKS readers to "play a stronger role in ensuring that our R&D and our educational offerings are suitably concerned with realistic stringent requirements" is appreciated [Letter From the Editor, ACM Software Engineering Notes, vol. 14, no. 6, October 1989, p. 2]. I often use RISKS examples in class (to demonstrate that the instructor is in touch with the world). In fact the current issue of SEN arrived in time to illustrate to a class the need for stringent requirements and testing. As if to underline the point, the following appeared on page A3 of the 1 December 1989 Asbury Park Press:

Computer Error Slashes JUA Surcharges: by Coleen Dee Berry

"Some 18,000 people who get their JUA automobile insurance policies through Computer Sciences Corporation may have thought their premiums were surprisingly less expensive this year.

"They were right.

"Due to computer error, CSC did not assess bad driver surcharges against about 18,000 of their policyholders. CSC is one of the four new computer companies hired to handle New Jersey Joint Underwriting Association policies.

"As a result, CSC has had to advance \$3.6 million to the JUA to cover the delayed payments, and last week began notifying those customers to expect a bill for the surcharges. ...

"The delayed surcharges were due to a glitch in the CSC's computer system during April and May, when the company was first taking over the JUA account.

...

"The move to computer companies was undertaken because it was thought to be cheaper and more efficient, according to state insurance officials."

I wonder if this "glitch" is any relation to the fellow who once stole Christmas? ...

Barry Kolb, Computer Science Dept., Ocean County College Toms River, NJ 08753  
(201) 255 - 0357

---

### **✂ Computerized voting machine misbehaves**

*Rodney Hoffman <Hoffman.ElSegundo@Xerox.com>  
5 Dec 89 09:20:22 PST (Tuesday)*

The 3-Dec-89 "Los Angeles Times" carried a story by Paul Houston headlined COMPUTERIZED VOTE TALLIES HAVE TOO MANY GLITCHES, EXPERTS CHARGE. The bulk of the story was a review of criticisms of these systems, pegged to last month's close gubernatorial election in Virginia. The article cited Mae Churchill of Los Angeles-based Election Watch, Computer Professionals for Social Responsibility, Roy Saltman (NIST) and Robert Naegele, a San Jose computer consultant.

The final paragraphs of the article related a miserable demo:

... one of Fairfax County's (VA) 600 Shouptronic machines fouled up in a demonstration for Los Angeles Times reporter William Trombley last May. "The machines have worked very well," Jane G. Vitray, secretary of the county board of elections, said as she prepared to demonstrate one of the machines to Trombley.

But the machine that prints out the names of candidates and issues -- the information that appears on the face of each machine -- printed everything in Italian. The ballot plotter also prints in French, German, and Spanish, as well as in English. "We didn't know it did that," Vitray said with some annoyance. "We didn't want that feature."

While an aide was left to deal with the language problem, Vitray and the

reporter moved on to the voting booth, where bells were chiming and red lights were blinking and an inviting green button at the bottom right corner of the machine said "vote."

"Don't push that," Vitray warned. "Once you push that, you can't vote for anything else. You only push that button when you're finished." In a previous election, a number of voters had pushed the green button too soon and then "called to tell us we were depriving them of their constitutional right," Vitray noted.

After Trombley finished voting, another red light came on to indicate that the result had been printed on a tape at the back of the machine. But when he and Vitray checked the tape, it was empty.

Vitray was exasperated. "I can't understand it," she said. "Everything worked so well last week, when the Girl Scouts were here."

---

### ✂ Re: Vote counting problems - experience in Michigan ([RISKS-9.50](#))

*Jeffrey R Kell <JEFF@UTCVM.BITNET>*

*Mon, 04 Dec 89 16:57:46 EST*

Some 15 years ago I worked the graveyard shift as a computer operator at a local service bureau. On two occasions we audited the city/county punched card tallies. Two (or more) members of the election commission brought the cards along with a tape containing the auditing/tallying software. The tape was IPL-ready for any generic IBM 360 to run standalone. It stacker-selected any multipunched cards as well as "spurious" punches which should be blank. Any cards munged by the reader were recreated and verified by the election officials.

Of course this does not solve the issue of missing/extra cards, write-ins, and other issues previously mentioned, but it does show that there was very little chance of our [the service bureau] tampering with or altering the results. The audit was done completely without interaction of the host site's software, operating system, or any other typical "hacking" paths.

Jeffrey R Kell, Dir Tech Services, Admin Computing, 117 Hunter Hall  
Univ of Tennessee at Chattanooga, Chattanooga, TN 37403

---

### ✂ Privacy issues raised about automating toll collection

*"Stephen W Thompson" <thompson@a1.quaker.upenn.edu>*

*Tue, 05 Dec 89 09:59:49 -0500*

Last night on "Market Place", a nightly half-hour program which is broadcast on one of the National Public Radio stations here, I heard a story reported by Joyce Miller about an Electronic Toll Collection (ETC) trial program in San Diego, California. ETC is intended to speed cars along crowded highways and still continue to collect tolls. The idea apparently involves placing a small (credit-card sized?) device on the car, which is then electronically sensed by

ETC equipment that then automatically bills the owner's account. As I understood the explanation, the driver doesn't need to stop (and maybe doesn't even have to slow down(?)). Drivers would pay a fee in exchange for the convenience, and traditional systems would never be phased out entirely.

Someone spoke saying that the system saves 15 seconds per car over traditional toll collection systems, which adds up when the roadways are crowded. There are 1000 cars in the trial program, which has been ongoing for several months (?). One participant was very pleased with the system.

The story included views by critics, who oppose the system because it is collecting information about drivers' driving habits, which they say could infringe drivers' privacy. One speaker said that ETC is particularly dangerous because the system is a government-controlled one.

I may have misunderstood that part, but it seemed that the critic wouldn't be as worried if the database of drivers' tolls were in the hands of a private company. I assume he was concerned with a greater opportunity for merging unrelated databases. (But a private company could misuse such data too, couldn't it?)

The reporter did not mention what authentication efforts are made. I don't know the method of sensing the ETC device (radio? optical? mag stripe?), but I wonder if there's any method of checking if device belongs to a particular car. If there is not, the devices might be very tempting to theives.

Anybody know anything more on this?

Stephen W. Thompson, 215-898-4585  
Institute for Research on Higher Education, University of Pennsylvania  
4200 Pine Street 5A, Philadelphia, PA 19104-4090

---

## **✂ Re: Electronic Interference in Fast Food Automation ([RISKS 9.50](#))**

*David Chase <chase@orc.olivetti.com>  
Sun, 03 Dec 89 17:08:27 -0800*

[McDonald's toaster voltage controls introduced zero-crossing transients, which fouled up clocks that count zero-crossings]

I'm surprised that this hasn't occurred somewhere else. The same technology that causes spikes in the toaster power regulator (triac or SCR switching) is also used in dimmers and other AC power regulators -- some of these available for home use. We used triacs in a home-made theater lighting controller some years ago, and it put some hellacious transients on the line.

For the circuit-phobic, an SCR is a three-terminal semiconductor device that has two states -- (1) don't conduct and (2) conduct (from positive terminal to negative terminal) until the current stops flowing on its own. The SCR is made to conduct by placing a small voltage on its trigger terminal while there is a forward voltage across its two main terminals. (A triac conducts in either direction, and is what we used, because it cuts the number of parts). These

devices regulate power very efficiently -- the triacs we used were rated to conduct up to 40 amps (RMS) with a maximum power dissipation of 40 watts (regulating "house current", that comes to 4600 watts).

In triac-based AC power controllers, the power is regulated by varying that amount of time that current flows. The triac will stop conducting each time the current passes through zero (120 times a second in this country), so what is actually controlled is how long to wait after a zero-crossing to turn on the power. For full power, you wait not at all; for little power, you wait almost 1/120 second; for 1/2 power you wait 1/240 second. When the power switches on (120 times per second), it tends to put a voltage spike on the line -- for large loads, and/or appropriate amounts of power, we found that it was pretty easy for the transient spike to cross all the way through zero (which, it happens, screwed up \*our\* zero-crossing detectors and made the lights flicker).

David

---

### ✂ Digital Cellular and the government

fritz <fritz@unocss..unl.edu>

29 Nov 89 18:14:07 GMT

An excerpt from an article entitled "Cellular Goes Digital" in the January 1990 issue of Popular Science, which discusses Digital Cellular, a new scheme using digital encoding and TDMA to allow three calls on one frequency:

Digital phones could also be used for what Sodha calls locational services. "With the time-division multiple-access system, you have the ability to measure the time it takes for a signal to go to a vehicle and back. That enables you to measure how far you are from the antenna tower," he says. What for? "You could pinpoint fairly accurately the location of a vehicle." The information could be used for navigation, or even to catch car thieves. "Your insurance might be cheaper if you subscribed to the service," Sodha suggests.

While I have no doubt that the information gained by such a system would be put to good use in combating crime, I do have my doubts as to how responsibly the government would use such information.

The article also mentions the fact that eavesdropping will be much more difficult since the transmissions will be digitally encoded and separated into discrete time slices. Although transmissions wouldn't be encrypted, special hardware would be required to listen in.

Is the trade-off worth it? Not to me. I'll trade the possibility of someone listening in on my boring phone conversations over the government possibly having ongoing information of my whereabouts any day.

Tim Russell Univ. Of Nebr. at Omaha russell@{zeus.unl.edu | unoma1.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 9: Issue 52

Friday 8 December 1989

## Contents

- [Unsafe French software?](#)  
[A. N. Walker](#)
- [Congress repeals catastrophic insurance, SSA still collects premiums](#)  
[Rich Rosenbaum](#)
- [Another runaway military computing project: WWMCCS](#)  
[Jon Jacky](#)
- [Courts say violation of professional code is malpractice](#)  
[Jon Jacky](#)
- [Risks of computerized typesetting](#)  
[Chuq Von Rospach from SF-LOVERS](#)  
[via Alayne McGregor](#)
- [486 chip faults: PC shipments halted, customers warned](#)  
[Jon Jacky](#)
- [Selling Government-Held Information](#)  
[Peter Jones](#)
- [Cellular phone service in Hungary](#)  
[Adam J. Kucznetsov](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✂ Unsafe French software

"Dr A. N. Walker" <[anw@piaggio.maths.nott.ac.uk](mailto:anw@piaggio.maths.nott.ac.uk)>  
Tue, 5 Dec 89 18:08:51 GMT

According to "The Sunday Correspondent" [a new `quality' weekly] of December 3rd, "Nuclear experts fear that reactors along the northern coast of France have fundamental design faults that could lead to a disaster which could devastate large areas of Britain. ... British experts are also concerned about the increasing reliance being placed by French nuclear engineers on computers whose tasks are so complex they can never be checked for safety. ..." (page 1).

The inside story, page 3, concentrates on engineering problems with the French PWR reactors, but there appear to be also some computer RISKS:

### "Key computer safety scheme error prone

French nuclear engineers are programming their computers using a language which is notorious for allowing dangerous errors to slip in, say British experts.

... Although computer equipment is now highly reliable, the incredible complexity of the software they [sic] run makes it very difficult to guarantee their behaviour ...

Professor John Cullyer, of Warwick University, ... says ... [the complexity] is "beyond present capabilities".

The French nuclear industry's wide use of a computer language called C is also criticised by [unnamed -- ANW] British software experts. They claim that it is too easy to write dangerous programs with C, yet difficult to spot the mistakes ....

[A French spokesman said ...] "Yesterday we had a demonstration for visitors and everything worked fine".

On the whole, I suppose I'm impressed that they use C rather than Fortran, Cobol, Assembler or BNF. Andy Walker, Maths Dept., Nott'm Univ., UK.

---

### **✶ Congress repeals catastrophic insurance, SSA still collects premiums**

*Rich Rosenbaum 226-5922 <rosenbaum@nssg.enet.dec.com>  
Tue, 5 Dec 89 16:38:16 -0800*

A story on "All Things Considered" (National Public Radio) this evening reported that although Congress has recently repealed the catastrophic illness law, the Social Security Administration (SSA) will be unable to stop collecting insurance premiums until June 3, 1990.

It seems that the SSA "warned" Congress that unless legislative action was taken by October 24, they would be unable to enact the changes quickly.

The problem?

"Apparently there are 150 different software programs that have to be changed and the computers just are not geared up to do that."

Once again, the computer is at fault. Interestingly, it is possible for the SSA to raise the premium in January to \$5.30.

By the way, people will eventually get their money back, without interest.

Rich Rosenbaum

---

### **✶ Another runaway military computing project: WWMCCS**

Jon Jacky <JON@GAFFER.RAD.WASHINGTON.EDU>

Thu, 7 Dec 1989 22:02:31 PST

This digest has carried occasional articles about problems with the WorldWide Military Command and Control System (WWMCCS). A history of the project since the early 1970's appears in the article, "The Pentagon's Botched Mission," by Willie Schatz, DATAMATION, Sept. 1 1989, pps. 22-26.  
>From the lead paragraph:

"Seven years after the (WWMCCS modernization) project started, the military has spent \$395.4 million, the users are outraged, the system is unfinished, responsibility for the project has been transferred, its name has been changed twice, and no one is entirely sure what will happen now."

- Jonathan Jacky, University of Washington

---

### **⚡ Courts say violation of professional code is malpractice**

Jon Jacky <JON@GAFFER.RAD.WASHINGTON.EDU>

Thu, 7 Dec 1989 21:54:52 PST

Here are excerpts from the article, Malpractice in IS? by J.J. Bloombecker in DATAMATION, October 15 1989, pp. 85 - 86:

A ruling by a US Court in Missouri ... recognized computer malpractice as the basis for holding third-party IS practitioners liable for acquiring an unworkable computer system for a client ...

In DIVERSIFIED GRAPHICS V. GROVES, the jury held consultants from Ernst & Whinney (Now Ernst & Young, having merged with Arthur Young and Co.) liable for shirking the Management Advisory Services Practice Standards of the American Institute of Certified Public Accountants (AICPA) in their procurement of a turnkey system for Diversified Graphics. In February, the US Court of Appeals of the Eighth Circuit agreed, and it let the jury verdict stand.

"DIVERSIFIED is a significant precedent for [establishing] the proposition that liability can be incurred by any professional performing the types of services that E&W offered to perform," says Peter Sadowsky, a partner in The Stolar Partnership in St. Louis, which represented Diversified Graphics. "It is equally likely to apply to people doing systems design or programming, not just systems acquisition." ...

"Prior to DIVERSIFIED GRAPHICS, most courts refused to extend professional liability standards to computer specialists. Now we've got a federal court of appeals doing just that," said J.T. Westermier, a partner in the Washington DC office of Fenwick, Davis and West, and a specialist in computer law.

Furthermore, says Westermier, an IS manager who lists membership in an association such as DPMA or ACM on a resume implies that he or she has accepted the associations professional standards. Having done that, a computer professional should expect his or her work to be judged by those standards.

Other lawyers who have analyzed the case, however, say it is unclear whether professional standards for IS managers could be used as a similar basis as the AICPA standards were in DIVERSIFIED.

John Hennelly, a partner at Bryan, Cave, McPheeters and McRoberts in St. Louis, which represented Ernst & Whinney, says the case doesn't necessarily lead to broader conclusions about the liability of nonaccountants ...

Eric Savage, with the Hackensack, N.J.-based law firm of Michael Goodman, believes it was easy for the court in DIVERSIFIED to find E&W guilty of malpractice because of the accounting organization's highly visible professional standards. Thus, he says, it would be difficult to apply the decision to a case that is adjudicating the liability of a computer professional not employed by an accounting firm. ...

(There are two sidebars to the story. One, labelled A CASE IN POINT, describes the client's needs, and how the system recommended by the accounting firm failed to meet the client's needs. This sidebar quotes the court's finding that the accounting firm did not have sufficient expertise to recommend a computer system for this client. Another sidebar, HOW SOME OF THE STANDARDS COMPARE, quotes the relevant portions of the AICPA Standards, which essentially say that members shall only accept jobs which they are qualified to perform, and shall conscientiously perform the jobs which they have accepted to the benefit of their client. This is placed alongside sections from the Association for Computing Machinery (ACM) Disciplinary Rules which essentially say the same thing.)

- Jonathan Jacky, University of Washington

---

### risks of computerized typesetting

*Alayne McGregor <alayne@gandalf.UUCP>  
Thu, 7 Dec 89 10:58:22 EST*

Date: Mon, 23 Oct 89 09:01:54 EDT  
From: Saul Jaffe (The Moderator) <sf-lovers-request@rutgers.edu>  
Sender: sfl@elbereth.rutgers.edu  
To: SFLOVERS-RECIPIENTS  
Subject: SF-LOVERS Digest V14 #339  
Reply-To: SF-LOVERS@rutgers.edu

SF-LOVERS Digest      Monday, 23 Oct 1989      Volume 14 : Issue 339

[...]

Date: 20 Oct 89 23:25:08 GMT  
From: chuq@apple.com (Chuq Von Rospach)  
Subject: Angel Station Typos

[[The following press release was distributed by Tor books about the typos in Walter Jon William's new book, Angel Station. If you are one of those who bought it and want a corrected copy, replacement instructions are

included.

How many publishers do \*you\* know that replace faulty books? Kudos to Tor...]]

For immediate release: 11 October 1989

#### THE STRANGE LUCK OF WALTER JON WILLIAMS

Not too long ago, Tor SF author Walter Jon Williams got a very pleasant surprise: His science fiction novel *HARDWIRED* (Tor, 1986) was prominently featured in a national advertising campaign for Nissan Motors' new "Infiniti" automobile.

Apparently the Powers that Be decided that some law of good fortune had been violated. When Williams returned from the World Science Fiction Convention in Boston to linger over the pages of his newest Tor hardcover *ANGEL STATION*, he got a most un-pleasant shock: Not only was there a rash of very strange typographical errors on page 9 of the book, but fully seventeen lines of type were completely missing from page 354.

When Williams called Tor's editorial staff in New York to report the errors, they immediately checked the press run of the book. Sure enough, the defects were present in every copy -- despite the fact that all previous proof sheets, and the book's bound uncorrected galleys, were free of the errors.

This isn't "business as usual" for Tor. Although an occasional typo slips by the proofreading process, and minor errors creep into final copies, nothing of this sort has ever happened to a Tor book before.

How did it happen? Well, no one knows exactly -- but the evidence points to some sort of software error in the generation of the final "repro proof" long after the stages at which books are normally checked and proofread in house. For example, the typos on page 9 all involve characters that are exactly five letters off in sequence from the correct characters.

Tor is offering to replace all defective copies of the *ANGEL STATION* hardcover with corrected copies from a new printing. To receive a correct copy, simply remove pages 1 through 6 (three leaves) and send them, along with your name and address, to Customer Service, St. Martin's Press, 175 Fifth Avenue, New York NY 10010, Attn: *ANGEL STATION* Replacement. This offer is open to individuals and dealers alike, though copies of the removed pages must be received for each copy the owner wants replaced.

Alternately, collectors who wish to keep their "true first" edition, typos and all, may write to Tor's own editorial offices at 49 West 24th St, New York NY 10010 for an errata sheet correcting the errors, which includes the missing text.

Meanwhile, Tor's editors are leaving nothing to chance where Williams's work is concerned. They've set up a special Walter Jon Williams Task Force to make sure the author's next work, a short-story collection called *FACETS* scheduled for publication as a hardcover in January 1990, escapes the

strange luck of Walter Jon Williams.

For further information, contact Patrick Nielsen Hayden, Administrative Editor, (212) 741-3100.

Chuq Von Rospach  
chuq@apple.com

---

### **✂ 486 chip faults: PC shipments halted, customers warned**

*Jon Jacky <JON@GAFFER.RAD.WASHINGTON.EDU>  
Wed, 6 Dec 1989 22:21:59 PST*

Additional news about problems with the 486 chip, noted by Peter Neumann in [RISKS 9.36](#), appear in a trade newspaper article, "Bug Hampers 486 Shipments" by Elliot M. Kass in COMPUTER DESIGN (News Edition) 28(2), Nov. 13 1989, p. 1:

Santa Clara, CA --- A Halloween fright spooked systems vendors late last month when a flaw was discovered in the floating point unit of Intel's 80486 micro-processor. The bug, unearthed by Compaq Computer (Houston, TX) during routine testing, could delay initial shipments of some 486-based systems up to two months.

Intel played down the seriousness of the design defect, saying it still plans to ship tens of thousands of the IC's this quarter. The firm reported that it had already fabricated a corrected version of the 32-bit microprocessor and that the first production quantities should be available by the end of the month. In the meantime, Intel has halted production of the flawed unit.

Intel declined to say how many of the defective chips have been shipped. Spokespersons insisted that the financial impact on the company would be minimal. The 486 was introduced this past April, and volume shipments began only recently. The manufacturers will accept returns from customers already in possession of the faulty IC's.

#### **NOT THE FIRST BUG**

Rumors about the bug had persisted for several weeks, according to industry observers. Confined to one small section of the IC unit, the flaws are neither serious nor unusual considering the complexity of the 1.2 million transistor device, most analysts agreed.

Most sources agreed that Intel's time frame for correcting the problem was realistic. On average, the redesign will mean one- to two-month ramp-up delays for 486-based systems, predicted Michael Slater, editor and publisher of MICROPROCESSOR REPORT (Palo Alto, CA).

Ironically, this is the second time that Compaq has detected a flaw in an Intel microprocessor. Four years ago the systems maker discovered a bug in the 486's predecessor, the 80386. That problem, which involved the production process, went undiscovered for 16 months after the unit had gone into full production,

and was very costly for Intel. This time around, Slater pointed out, the bug is confined to a small aspect of the chip's design, and was picked up a few weeks into production.

Compaq, which came across the problem during beta tests of its newly announced Deskpro 486/25 personal computer, admitted that it in its present state, the 486-based PC's weren't ready for market. The new processors will heavily target CAD and other technical applications dependent on the 486's floating point math processor. The microprocessor unit's design flaw reportedly involves the simultaneous execution of tangent and sine or cosine functions, as well as certain error detection features. General purpose business programs that don't make use of the FPU could still run unhindered.

As of press time, Compaq was still uncertain how the shipping schedule for its new machine would be affected, but said it was confident they would be in production quantities by the first quarter of next year.

#### VENDORS MODERATELY AFFECTED

The effect of the chip defect on other vendors varied. IBM (Armonk, NY) the only vendor that's already begun shipping a 486-based product, suspended shipments of its 486/285 Power Platform. Company spokespersons said they would instruct customers already in possession of the board to limit its use to test environments, or to applications that don't involve the affected portions of the chip.

IBM said it expects to resume shipments of its processor board early next month. The company is continuing production of the Power Platform with the original chips and will replace them once the debugged units are available. The substitution procedure is relatively simple, the vendor noted, and will prevent further slipping of its shipment schedule. Customers in possession of the boards will receive an upgrade.

- Jonathan Jacky, University of Washington

---

#### **✖ Selling Government-Held Information**

*Peter Jones <MAINT@UQAM.bitnet>*

*Wed, 6 Dec 89 08:20:17 EST*

On CBC's Daybreak program this morning, there was an interview about the possibility of selling information help by government institutions to private companies. For example, names and addresses of municipal bondholders or property owners could be used for direct mailing.

Currently, there is a dispute concerning the information held by the Inspector of Companies on company names, and names and addresses of directors. This information, although publicly available, is regarded by the Inspector as confidential. For example, it would be possible to guess a person's political affiliations from the presence of his name on the board of directors of a political organization.

There are two issues here, being disputed by the private companies on one side, and the government and the Quebec Civil Liberties Association on the other:

- 1) Prevention of access to confidential data. (A straightforward computer problem).
- 2) Making data available in a form that allows massive searching and matching.

This raises the privacy issues currently being disputed.

Peter Jones    MAINT@UQAM    (514)-987-3542

---

## **Cellular phone service in Hungary**

*Adam J. Kucznetsov <adam@cunixf.cc.columbia.edu>*

*Tue, 5 Dec 89 17:19:48 EST*

From New York Times (5 Dec. 1989) business section (excerpts):

### US West in Budapest phone deal

US West Inc., one of the nation's seven regional Bell telephone companies, said yesterday that it had signed an agreement with Hungary to build a mobile cellular telephone system in Budapest.

The Hungarian cellular system will be the first such telephone network to be constructed in Eastern Europe. Because of the shortage of telephones in the nation, Hungarians are expected to use cellular telephones for basic home service, as well as mobile communications.

For Hungary and the other Eastern European countries, which have antiquated telephone systems, it will be faster and cheaper for the Government to deliver telephone service by cellular networks than it would be to rebuild the nation's entire telephone infrastructure.

[one paragraph omitted]

The system, which is scheduled to go into operation in the first quarter of 1991, will initially provide cellular communications to Budapest's 2.1 million residents. Eventually, the system will serve all of Hungary, which has 10.8 million citizens.

[rest of article omitted]

The article explains that "[the system is] viewed as an alternative until the country can develop its infrastructure" and goes on to state that "Hungary currently has 6.8 telephone lines for every 100 people" compared to 48.1 in the United states.

Hungary's interest in supplanting an antiquated and inadequate phone system is understandable. The privacy issues, however, raised by a proposal to make (presumably unencrypted) cellular telephone service one of the primary communication channels of the country -- even in transition to a more capable conventional system -- should be obvious to RISKS readers.

Adam J. Kucznetsov, Department of Linguistics, Columbia University  
{ajuus@cuvmb.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 9: Issue 53

Monday 11 December 1989

## Contents

- [Computerized public records boon to private eyes probing suitors](#)  
[Jay Elinsky](#)  
[Jon von Zelowitz](#)
- [Should computers be legally responsible?](#)  
[A. Lester Buck](#)
- [Automatic toll systems](#)  
[Jerry Harper](#)
- [Software Development](#)  
[Bill Murray](#)
- [Newsgroup posting rejected, rejected, rejected, ...](#)  
[Earle Ake](#)
- [Comments on Unix INDENT program](#)  
[Simson L. Garfinkel](#)  
[Nick Lai](#)  
[David McAllister](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **Computerized public records boon to private eyes probing suitors**

"Jay Elinsky" <ELINSKY@YKTVMZ.BITNET>  
Sun, 10 Dec 89 21:44:06 EST

>From "Boy Meets Girl, '89, Can Be a Detective Story" by Dirk Johnson, in  
the New York Times, 10-Dec-89, Page 1:

"Computerizing of public records in recent years has proved a boon to investigators, who say they can find out almost anything simply by keying a Social Security number into a computer... `It's usually very easy', said Ed Pankau, the president of Inter-Tect [a Houston investigative agency], who is the author of `How to Investigate by Computer'."

The context of the article, from the lead paragraph: "Eager to trust but determined to verify, many single women in this age of risky romance are hiring private detectives to check the backgrounds of their suitors." A few

paragraphs later, "Women are far more likely than men to hire an investigator, and usually their suspicions are on the mark, detectives said."

In this case I'm tempted to call easy access to records (assuming it's legal) a benefit instead of a risk. Then again, I got married ten years ago, and my fiancée's investigation of my background was more traditional, like meeting my parents and using her "feminine intuition". And the article ends with a non-computer-related risk: The woman who is the subject of the article had three men investigated and found "skeletons in their closets". The fourth man she investigated was a-ok, and she was so thrilled that she told him he had passed the investigation. He wasn't thrilled to hear that he had been investigated. "He kind of freaked out", she said. "But then, as I tried to explain why I did it, he understood, kind of". She added, "We're not dating anymore."

Jay Elinsky, IBM T.J. Watson Research Center, Yorktown Heights, NY

---

### **✶ Don't Give Social Security Numbers to Girlfriends**

*Jon von Zelowitz <vonzelow@adobe.com>*

*Mon, 11 Dec 89 00:10:10 PST*

[...] For \$500, the Inter-Tect investigative agency in Houston promises to verify within a week a person's age, ownership of businesses, history of bankruptcies, if there are tax liens, appearance in newspaper articles, as well as divorces and children. Some clients have paid the detective agency as much as \$10,000 to unearth secrets.

"People want to find a quality partner," said Mr. Pankau, who is a former investigator for the Internal Revenue Service. [!-jvz] "I wouldn't say they're paranoid, but they're very cynical."

...sun!adobe!vonzelow vonzelow@adobe.com Jon von Zelowitz

---

### **✶ Should computers be legally responsible?**

*A. Lester Buck <buck@siswat.UUCP>*

*11 Dec 89 07:21:12 GMT*

Recently I ran across a copy a paper in my files entitled "Are There Senses in which a Computer may Properly be Held Responsible for its Actions?" by J.P.A. Race from Brunel Univeristy, UK, in the volume "Information Technology for the Eighties", ed. R.D. Parslow (Heyden,1981). I include some extended excerpts from his article. Several of the points Race proposes have fascinating RISKS implications, and I would be quite interested in more recent references on this subject. I also have not yet heard of insurance policies for the actions of a computer. Do such policies exist?

"...at the moment our natural reaction [to a wrong brought about by the agency of a computer], to say 'It was the computer's fault', will be laughed at. The sophisticated will [...] turn immediately to the human being involved, the

programmers, operators, compiler writers, maintenance engineers, sponsors, consultants, hardware designers... and try to apportion liability among them."

"Such critics of our 'It was the computer's fault' are themselves naive. We are quite quite correct in our instincts to start by blaming the computer, for the following reasons:

"The computer system may be indeed liable, and no one else. The program may have been correctly designed and arranged to adapt to circumstances, but on this occasion the adaptation led it astray. The human beings involved acted in good faith to the best of their ability, and are not liable. Yet a blame-worthy thing happened. Therefore the non-human system must be blamed, unless we call the happening an Act of God, which we would never do if a human being had been involved instead of a computer.

"The computer system may evade responsibility wholly or in part, because of negligence or deliberate action on the part of one or all of the human beings involved. But we have to start somewhere, and by calling to account the agent -- the computer -- which is prima facie responsible, the process of finding a culprit fails safe. We shall see later how the computer may be expected to defend itself by inculpating others, and how it can make amends if found wholly or partly liable.

Race defines a "computer system" as "one particular combination of hardware, software, and data, such that its functional behaviour is different from any other system", the data being particularly important to distinguish between initial identical twins that have experienced different learning sets for their expert systems. He then draws a distinction that a responsible computer is not at all the same as an "intelligent" computer. "No, the characteristic of the computer systems under discussion is not so much intelligence, as the ability to rationalise, that is, to give an account of their actions, and to construct courses of action using powerful planning procedures, like Terry Winograd's SHRDLU..."

"We are talking about responsibility: no need to put [the computer system] to Turing's test to show a human level of intelligence. In fact, as pointed out by Turing's brother, a computer like [this responsible system] will make a poor showing at writing a sonnet, but that doesn't stop us from treating it as a responsible agent. Few submarine captains write good sonnets either, or clerks, or public corporations, yet all these entities have responsibilities in law."

"There are three aspects of punishment:

Retribution: the need for society to get its revenge on the wrong-doer: a basically irrational (but quite understandable) emotional response. If this means pushing a computer system over a cliff after it has driven someone to suicide through sending them wrong electricity bills, we can understand it. [...]

Rehabilitation: In this sense, the aim of punishment is to improve the individual for his own sake and that of society. In the case

of a computer, this may involve re-programming or the indication to the computer that its previous response had been wrong, so that this reprimand is stored as a new parameter value to adjust its future behaviour. The fact that we did not use a cat-o'-nine-tails or the brig does not mean what we did was not punishment, any more than it is not punishment - of a severe kind - if a court-martial reprimands an officer who runs a frigate aground.

Deterrence: The fact that [this computer system] is punished should be communicated to other computer systems working on similar things. [...]

"Lastly in this section we should consider the case where a computer is involved as a principal in a civil suit: punishment is not involved, but restitution of damages is. In the past one would have thought it bizarre for the mechanical agent to be the actual defendant, yet as was said at the outset, our big problem with computers is that unlike hammers, it is very hard for a plaintiff to find any human being to accept responsibility for their bad behaviour. So he should be able to sue them, just as a corporation may be sued, and for much the same reason.

#### "PROPOSALS

Computer systems should be designed to include the ability to give an account of the bases of their actions, as 'expert systems' do now, and, at a more mundane level, commercial systems do with an inbuilt 'audit trail'.

Our instinct to 'blame the computer' when it makes errors should be elevated to a policy. It should be possible to take civil or criminal action against it in circumstances in which a human agent would also have been taken to court.

Based on the system's own account of events, and other evidence, responsibility will be assigned and judgement given.

Where the responsibility is laid at the computer's door, the basis for its behaviour (program or data) will be altered.

To provide for restitution of damages when a system is successfully sued in a civil action, it should not be a 'man of straw' but would hold money reserves or insurance."

A. Lester Buck    buck@siswat.lonestar.org ...!texbell!moray!siswat!buck

---

#### Automatic toll systems

*Jerry Harper <jharper@euroies.ucd.ie>  
Fri, 8 Dec 89 19:33:16 GMT*

An automatic toll system is currently in operation in Southern Norway,

installed by Philips if my memory serves me adequately. The system is extremely straightforward in operation. Regular users of the road simply buy a playing-card sized reflective disk which is mounted on the nearside rear window. As a vehicle approaches the toll point it passes over a sensor (a loop, I think) which activates a low intensity microwave transmitter. A beam from the transmitter strikes the upper nearside of the vehicle and a proportion of rays are reflected from the disk onto a receiver. Now as each reflective disk has the ID of the vehicle owner embossed on it the reflected pattern also presents the ID and thus beginning and endpoints of a journey on a toll road can be accurately determined. Furthermore, if the system receiver fails to register an ID a video camera is activated which photographs the backend of the suspect vehicle. The owner can then be traced through the license plate. Road users can be either billed every month directly or may pay a certain amount in advance. Vehicles can pass through the electronic "gate" at up to 70kmh with detection accuracy of ID remaining up in the early nineties (?) (I am quoting from memory but I remember being stunned by the figures at the time). Only extreme environmental conditions affect the system adversely (micro wave is not as sensitive to climatic changes as infra-red radiation). How do I come to have this knowledge? Well, we are designing an automated policing system here which should keep us busy for a few years.

John G. Harper, Computer Science Dept., University College, Dublin 4, IRELAND

---

### **✂ Software Development (Re: Curtis Jackson, [RISKS-9.50](#))**

<WHMurray.Catwalk@DOCKMASTER.NCSC.MIL>

Sat, 9 Dec 89 12:14 EST

Curtis Jackson writes in [RISKS-9.50](#):

>We insisted on writing the design spec before writing any code, and  
>finalizing the design spec (after initial review) down to the  
>individual bit level. We then wrote pseudo-code for all modules, and  
>peer-inspected those. Finally we wrote the code with strict commenting  
>standards and assembled it, then peer-inspected that. Finally we wrote  
>module tests, simulated those, then string tests, simulated those, and  
>one day the hardware was off the drawing boards and in the lab.

Note the order in which code and test data were prepared. (Note also the two "finally"s.)

This scenario illustrates part of the problem that we have in software development.

Test data are part of the specification and the acceptance criteria of any product. In all other engineering activities they are prepared before, rather than after the product. In software, not only are they prepared after the product, but often as an after thought. For the most part, they are prepared by the same person as produced the code. Thus, the product exits test "when the programmer can no longer find anymore of his own errors."

Before any one tells me that you cannot prepare the test data until after the code because you do not know what either will look like until the code is

written, let me say that I have heard that argument before. My answer (retort) is that if you started preparing the code before you knew what the product would look like and exactly how it will behave, then you clearly started too soon.

Now the contributor quoted clearly thought that he and his colleagues were proceeding in a rigorous and disciplined manner, in accordance with the very best of practice. That their practice could be so far from good engineering practice is evidence of how far we have to go.

Note that he said nothing about building a prototype. How would you like to fly in an airplane built to a new design that did not include a prototype? (Do not build a plane without a prototype; do not fly passengers in the prototype.)

How long will we tolerate this practice and the quality that results. Must we reinvent engineering? Are we so wrapped up in our own mythology and metaphors that we cannot learn from other disciplines?

William Hugh Murray, Fellow, Information System Security, Ernst & Young  
2000 National City Center Cleveland, Ohio 44114  
21 Locust Avenue, Suite 2D, New Canaan, Connecticut 06840

---

### **✘ Newsgroup posting rejected, rejected, rejected, ...**

*Earle Ake <fac2@dayton.saic.com>*

*11 Dec 89 12:57:50 EST*

There is a new newsgroup that I subscribe to called vmsnet.announce.newusers. I decided to post a message to it. That is when the fun began. The newsgroup is unmoderated. After I posted to the newsgroup, I received a mail message from a site scolding me for posting to a moderated newsgroup and told me to post directly to the moderator instead. He is a copy of the message.

"This newsgroup is moderated, and cannot be posted to directly. Please mail your article to the moderator for posting."

It then included my original message to make sure I knew what I had done.

I was going to ignore it until I received 5 more messages from the same site complaining about the same message. I started to wonder, do we have a loop here? I fired a message off to the postmaster at the offending site to stop the messages. A day past and no reply. The messages kept coming in. I started to keep track of how many and how often they were mailed. They were mailed every half hour since I first posted the message. I then looked up the administrators name in the UUCP maps. I sent him a message directly to have him stop these things. He responded by saying he wasn't sure what was happening and to send him a sample of the message so he could fix it. Now we are up to 85 messages. I finally got a response from him saying he had shut them off. It seems one of the sites that he is connected to accepted the message and then tried to hand it off to his site. His version of NEWS thinks that any newsgroup that has the word 'announce' in it IS MODERATED no matter how you have it set up! The remote

site tried every half hour to hand the message off to his site. His site would in turn reject the message and send a nasty gram back to me. We finally got all this straightened out after 140+ messages bounced back to me. I don't think I will post to that newsgroup in the near future!!!!

Earle Ake fac2@dayton.saic.com uunet!dayvb!fac2

---

### **comments on Unix INDENT program (Lai, [RISKS-9.50](#))**

*Simson L. Garfinkel <simsong@prose.CAMBRIDGE.MA.US>  
Wed, 6 Dec 89 3:43:25 EST*

Actually, indent is merely changing the old-style C code (`x -= 1`) to the new style. (`x = 1`). Careful programmers always put in whitespace between assignment and variables for this reason. Some compilers will flag (`x=-1`) as a warning because it is ambiguous.

Careful programmers also always use lots of parens to make their intentions clear. such as `((x<3) && (y>2))`.

---

### **More on indent**

*Nick Lai <lai@east.Berkeley.EDU>  
Wed, 6 Dec 89 08:29:02 PST*

Of course. I alluded to the old style / new style conversion (K&R A.17) in my previous note.

I am a careful programmer. The whole point is that sometimes I run across code written by idiots who insist on two-space indentation, no spaces between elements of comma-separated lists ("`x=foo(9,34,&hoho)`"), and writing code like "`int x=-1`". Indent held out the promise of being able to convert that crap into something readable. But it was just a boulevard of broken dreams.

Nick

---

### **Problem with indent revisited**

*David McAllister <dmcallis%albion@cs.utah.edu>  
Mon, 11 Dec 89 15:03:16 -0700*

Just so you know, the problem with indent swapping "`x = -y`" to "`x -= y`" also works with "`x = *y`" to "`x *= y`"  
Pretty silly, huh?

DMc



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 9: Issue 54

Tuesday 12 December 1989

## Contents

- [Mariner I \[once more\]](#)  
[Mark Brader and Fred Webb](#)
- [Re: Software tool \(indent\) munges code](#)  
[Mark Moraes \[2x\]](#)  
[Joe Dellinger](#)  
[Amos Shapir](#)
- [Re: SSA software maintenance](#)  
[Dan Franklin](#)
- [Re: Don't Give Social Security Numbers to Girlfriends](#)  
[Will Martin](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **Mariner I [once more]**

*Mark Brader <msb@sq.sq.com>*

*Tue, 12 Dec 89 02:53:54 EST*

The new Usenetoid newsgroup alt.folklore.computers (a.f.c) has been having a discussion of the Mariner 1 space probe failure in 1962 due to a missing "-" (Arthur C. Clarke: "The most expensive hyphen in history." The vehicle cost \$18,500,000.) which was discussed at length in Risks in November and December 1987.

As was discussed in Risks, a popular but apocryphal version of this story -- even appearing in computer textbooks -- is that a "." was substituted for a "," in a FORTRAN DO statement, converting it to an assignment. But no contemporary evidence was ever cited to support that story.

Now the a.f.c discussion began with exactly that apocryphal story; someone has posted the old Risks discussion to clean that up. But this time one thing is different. Someone else has posted giving a likely explanation of the FORTRAN DO version of the story. Notice, by the way, that it did not cost even one spacecraft, let alone the billion dollars claimed in one of the textbooks.

Fred Webb (fwebb@bbm.com) writes in alt.folklore.computers:

Subject: Fortran story - the real scoop

Summary: I was there!

...

This kind of thing is a common Fortran bug, so there are probably many different stories going around with a similar theme. Some of them are probably true. I do know of one such instance that really did happen, at Nasa.

I worked at Nasa during the summer of 1963. The group I was working in was doing preliminary work on the Mission Control Center computer systems and programs. My office mate had the job of testing out an orbit computation program which had been used during the Mercury flights. Running some test data with known answers through it, he was getting answers that were close, but not accurate enough. So, he started looking for numerical problems in the algorithm, checking to make sure his tests data was really correct, etc.

After a couple of weeks with no results, he came across a DO statement, in exactly the form ... indicated above. After changing the . to a , the program results were correct to the desired accuracy. Apparently, the program's answers had been "good enough" for the sub-orbital Mercury flights, so no one suspected a bug until they tried to get greater accuracy, in anticipation of later orbital and moon flights. As far as I know, this particular bug was never blamed for any actual failure of a space flight, but the other details here seem close enough that I'm sure this incident is the source of his version of the story.

Sent to Risks by Mark Brader, SoftQuad Inc., Toronto

[See [RISKS-8.75](#) for the missing `bar' in `R dot bar sub n' expression that contributed to the loss of Mariner I; details from Paul Ceruzzi. PGN]

---

### **🔥 Re: Software tool (indent) munges code**

Mark Moraes <moraes@csri.toronto.edu>

Tue, 12 Dec 89 21:45:30 EST

In [RISKS-9.50](#), lai@east.Berkeley.EDU (Nick Lai) comments that indent has an insidious bug under BSD and SunOS. He is wrong about the bug under BSD and SunOS, right about the bug if his compiler is ANSI compliant, but definitely right in pointing out the risk.

- On Unix systems, pcc derived C compilers will interpret that code exactly as indent did, generating a warning in the process, so indent's behaviour would not change the intent of the code. (Like the compilers, indent should probably warn the user) Therefore, for old

style C, indent's behaviour is NOT wrong. Most old compilers would have treated that code the way indent did, so indent just made the code clearer.

- With ANSI C compilers, the `=op` style syntax is obsolete. This is one of the QUIET CHANGEs in the proposed ANSI C standard -- see section 3.1.5 (Operators) of the Rationale (my copy is dated Oct 31,1988 -- the section number may have changed since)

So, if the programmer wrote

```
x=+1;
```

ANSI C compilers would interpret this to mean "assign the value +1 to x". (GNU C version 1.34 on a Sun3 interprets it this way \*EVEN\* with the -traditional flag)

K&R1 C compilers would interpret this to mean "increment x by 1"

pcc derived compilers also complain with something like:

"foo1.c", line 7: warning: old-fashioned assignment operator

"foo1.c", line 9: warning: ambiguous assignment: assignment op taken

I don't know if other K&R1 compilers complain this way.

(Note that Ultrix 3.1 compilers also follow K&R1 and complain)

indent as distributed with BSD and SunOS silently assumes K&R1 C behaviour and converts it to

```
x += 1;
```

GNU indent version 1.1 assumes ANSI C behaviour and converts it to

```
x = +1;
```

Ultrix 3.1 indent does this too (even though their compiler still follows K&R1!)

People converting programs from old C to ANSI C should check all code (using grep or some similar tool) to make sure sequences of the form "`=op`" are converted to "`= op`" or "`op=`" depending which is meant! (And make some suggestions on programming style to the person who wrote the code originally)

### Re: Software tool (indent) munges code

Mark Moraes <moraes@csri.toronto.edu>

Wed, 13 Dec 89 01:29:49 EST

Beverly Erlebacher <erlebach@turing.toronto.edu> points out that SunOS4.0 compilers also follow ANSI, and interpret `=op` as `= op`, compiling silently if `op` is a unary operator. But SunOS4.0 indent works like SunOS3.x/BSD indent and indents according to the old rules, making it `op=`. So for SunOS in my previous note, please read SunOS3.x.

### Fun and Games with Indent

Joe Dellinger <joe@hanauma.stanford.edu>

Wed, 13 Dec 89 02:54:02 PST

You think the fun and games with statements like "x=-5;" are bad? It is MUCH worse than that! Here is how the following line of code mutates with each successive application of 4.3BSD lint (this happened to me):

Original: x = .5;

A typical piece of C code from a scientific application.

1st iter: x =.5;

Uh... still valid, but NOT an improvement.

2nd iter: x .= 5;

Now it's a syntax error!

Converged: x.= 5;

At this point it's stable: a good-looking valid piece of code has become a bad-looking syntax error!

Fortunately Convex's "lint" has these bugs fixed. It's a very useful tool, WHEN IT WORKS.

---

### ✂ Re: comments on Unix INDENT program (Lai, [RISKS-9.50](#))

Amos Shapir <amos@taux01.nsc.com>

13 Dec 89 16:32:47 GMT

Simson L. Garfinkel in [RISKS-9.53](#) writes:

>Actually, indent is merely changing the old-style C code (x -= 1) to the new  
>style. (x = 1). Careful programmers always put in whitespace between  
>assignment and variables for this reason. Some compilers will flag  
>(x=-1) as a warning because it is ambiguous.

This case is a typical example of what RISKS is all about: the purpose of "indent" is to change/add \*white space\* so the outcome is nicer and more readable; it has no business "merely changing" the code in a way that might change its meaning.

Since in old-style C the term (x=-1) was ambiguous, "indent" may issue a warning or do nothing, but not try to guess which of the possible ways to add blanks is the correct one, and certainly not rewrite it without indicating in any way that it did.

Another aspect of RISKS is that in this case "indent" was run on a program written in new-style C, in which that term had only one meaning - which is different from the one assumed. In essence, "indent" was used to process input written in a language different from the one it was designed for, but similar enough to confuse an innocent user.

Amos Shapir, National Semiconductor (Israel) P.O.B. 3007, Herzlia 46104, Israel

---

## **✉ Re: SSA software maintenance**

Dan Franklin <dan@WILMA.BBN.COM>

Tue, 12 Dec 89 0:00:43 EST

The news about the SSA being unable to reprogram its computers in time for the catastrophic health care bill repeal comes as no surprise to anyone who's read "Nations at Risk: the Impact of the Computer Revolution" by Ed Yourdon (1986, YOURDON Press).

Indeed, the SSA problems are not unique, and are no reflection on the energy, talent or dedication of its staff -- but rather the accumulation of old hardware, old software, and a general lack of understanding on the part of Congress of the difficulties of dealing with massive volumes of data. For the SSA, massive means 446 billion [bytes] of disk storage to service 650,000 inquiries each day. It means 113 tons of computer printouts per month; 380 million wage reports per year, and 40 million checks per month. As former commissioner John A. Svahn says, only a "daily miracle" gets the monthly checks out on time. Having worked with the SSA computer people, I can personally testify to their enormous energy and professionalism, and I firmly believe that the \$478 million five-year modernization program approved by Congress in 1982 will eventually (though not in five years) get the organization back in control.

The demurral about the time needed has unfortunately now been vindicated.

There's more on p. 432:

- o Calculating the cost-of-living increase for 50 million recipients of Social Security benefits takes 20,000 hours of computer time on older computer systems within the SSA. [That's 1.44 seconds per recipient!]
- o When the SSA upgraded its computer systems in 1981 from five-digit checks to six-digit checks, it required 20,000 man-hours of work and 2,500 hours of computer time to modify 600 separate computer programs.
- o The morale in the SSA maintenance group was so bad at one point that one of the programmers was caught urinating on a disk pack...

Before you laugh too loudly at this, remember that the SSA has one of the better MIS organizations in the country. They deal with gargantuan volumes of data, and they work in a political environment that defies imagination -- but they get the job done, and they get the checks out each month...

True, an incorrect check is lots better than no check at all!

These passages are used to help illustrate one of the book's points, which is that large information systems all over the U.S. are suffering badly, and that problems with these systems are a significant factor keeping us from being more competitive. He makes a persuasive case; the book is worth reading (though redundant towards the end).

Dan Franklin



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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 9: Issue 55

Monday 18 December 1989

## Contents

- [Risks of Mail \(the "yellow peril"?\)](#)  
[Joe Dellinger](#)
- [PR RISKS of computer communications -- Prodigy](#)  
[Mark Jackson](#)
- [Re: private eyes probing suitors -- Amazon Women on the Moon](#)  
[Dwight McKay](#)
- [Faults in 29000 RISC chip](#)  
[Jon Jacky](#)
- [The Trojan horse named "AIDS"](#)  
[contributed by many who are not neigh-sayers](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **✉ Risks of Mail (the "yellow peril"?)**

*Joe Dellinger <joe@hanauma.stanford.edu>*  
*Thu, 14 Dec 89 03:01:06 PST*

Several computers in the Earth Science department at Stanford were brought to their knees Dec 13 by an interesting combination of bugs. I can only assume similar numbers of machines around campus in other departments also succumbed. I don't really know, because our network is dead as a result of it!

For some reason, the Stanford Chinese Student association mailing list started bouncing mail infinitely between two Stanford machines, "Macbeth" and "Portia". At each iteration the 30K of mail was rebroadcast anew to everyone on the list, including at least one Chinese student on each machine in our department. This was the first bug. I don't know why it happened. (Anyone know that story?) This bug alone would have been bad, but not catastrophic...

The problem was that after each successive bounce the return address got longer and longer, until monstrosities like the following became commonplace:

<@Macbeth.Stanford.EDU,@Portia.stanford.edu,@Macbeth.Stanford.EDU,@Portia.stanfo

rd.edu,@Macbeth.Stanford.EDU:xu@spanky.Stanford.EDU>

Once the reply addresses got up to about the length shown in this example, they started to overflow a fixed-length buffer in all Berkeley-derived mails (NO checking for overflow, OF COURSE). This caused the affected mail processes to go crazy. First of all they sent an error message back to the sending machine (causing it to send the viral mail \_again\_ 30 minutes later). Worse, the mangled mail processes continue to run forever until somebody kills them. (And it takes kill -9 as superuser to do it.) One such mail process on a lightly-used Earth Science machine accumulated \_9500\_ minutes of CPU before anyone figured out why the machine had been so slow for the preceding week!

Our first reaction was to scream at the people who run the list, and they said they fixed the problem, but their fix only resulted in a greater variety of mail loops being generated; various interesting orbits about portia, polya, hamlet, macbeth, ...

Needless to say as the traffic built up the CPUs and then finally the network itself in the Earth Science department ground to a halt. It became impossible to even log in to many machines to kill the offending mail processes. Killing the processes wasn't very effective, either, since that would not stop Macbeth from immediately starting the whole mess up again. We finally pulled the plug on sendmail.

Fortunately this evening Stanford had a power glitch that seems to have crashed most of the offending machines, so the network is OK again now. :-)

---

### ✂ PR RISks of computer communications

<MJackson.Wbst@Xerox.COM>

14 Dec 89 07:33:07 EST (Thursday)

The following is extracted from a brief item, "Prodigy service creates controversy," on the business page in Wednesday's /Democrat and Chronicle/ (Rochester, NY). It appears that when you're "where America shops," discussions about who America might be make you nervous. . . Mark

> There are better ways to get publicity, but a fight between homosexuals and  
> Christian fundamentalists nevertheless has called attention to the rapid  
> growth of a home computer service owned by IBM and Sears.

> The Prodigy service has expanded to a quarter-million subscribers in  
> 160,000 homes from 30,000 homes a year ago. It serves 21 of the nation's  
> largest markets, up from six a year ago.

[business stuff deleted]

> Prodigy's adverse publicity came this week after it cancelled a chat  
> service named Health Spa, a "bulletin board" that allowed subscribers to  
> post notices or communicate on health-related issues.

> Prodigy said Health Spa was canceled because of low usage, but some

> subscribers said it was because one section of Health Spa turned into a  
> forum for a heated debate on homosexuality between gays and fundamentalist  
> Christians.

> Dozens of subscribers have been demanding the return of Health Spa - an  
> unintentional testament to the popularity of Prodigy's service.

---

**✂ Re: private eyes probing suitors -- Amazon Women on the Moon**

*<mckay@harbor.ecn.purdue.edu>*

*Thu, 14 Dec 89 15:45:11 EST*

There's an amusing but scary skit in the movie, "Amazon Women on the Moon" regarding a women who checks out her boyfriend.

On a blind date, he arrives at her place. She asks for his driver's license and a valid credit card. She walks over to her desk and runs the credit card through a magnetic strip reader (like at a store) and gets a printout of all the other dates he's had and how they turned out...

Dwight D. McKay, Engineering Computer Network Workstation Software Support,  
Purdue University,

---

**✂ Faults in 29000 RISC chip**

*Jon Jacky <JON@GAFFER.RAD.WASHINGTON.EDU>*

*Thu, 14 Dec 1989 13:51:45 PST*

Here are excerpts from an article in the trade publication ESD: THE ELECTRONIC SYSTEM DESIGN MAGAZINE, Nov. 1989, p. 22:

"Stepping on 29000 Bugs," by Michael Slater

The current stepping of Advanced Micro Devices 32-bit RISC processor, the 29000 revision D, still has three acknowledged bugs. However, the bugs are all relatively minor. They consist of an instruction burst mode problem, an exception handling priority error, and a data-access exception problem.

Since hardware workarounds have been required for the instruction burst mode problem since the first silicon, existing designs either already incorporate the fixes or don't produce the offending set of conditions. Modifications to the exception handlers can correct the other two bugs. These same bugs were also present in revision CA. The most serious bug from revision C, the failure of the branch target cache to work reliably, has been fixed.

(Here follow many column-inches describing the problems and workarounds in more detail.)

AMD has distributed samples of the new revision, and current orders are expected to be filled with this revision.

- Jon Jacky, University of Washington

---

## **✂ The Trojan horse named "AIDS"**

*Evan "Biff Henderson" Eickmeyer <eickmeyer@girtab.usc.edu>  
Sat, 16 Dec 89 02:14:52 PST*

The following article is from the Los Angeles Times, 15 December 1989, p.D3.

AIDS Data Disk Has PC-Damaging Virus, by Michael Specter, The Washington Post

A mysterious computer diskette about AIDS that was mailed to major corporations, insurance companies and health professionals across the world contains a hidden program that has destroyed information in thousands of personal and corporate computers, police in London said Thursday.

Officials of Scotland Yard said at least 10,000 copies of an unusual "AIDS Information Diskette," which promised to help users deduce their risk of becoming infected with the AIDS virus, were sent to people in England, Scandinavia, Africa and the United States.

Hospital systems from London to Stockholm reported damage Thursday and AIDS researchers at major institutions in the United States, from the National Institutes of Health to the University of California at San Francisco, issued alerts to all their computer users.

"Extremely urgent message for all National Institute of Allergy and Infectious Disease PC Users," said a flyer sent Thursday to AIDS researchers at NIH. "A diskette from PC Cyborg Corp. contains a highly destructive virus. All systems running these programs had ALL hard disk data DESTROYED." Neither that corporation nor Ketema Associates, its parent company, has any known officers or location, according to people who tried Thursday to find them.

In Sweden, the State Bacteriological Laboratory sent letters to clinics and doctors warning them of the diskette. Chase Manhattan Bank was one of the first companies to report problems with the diskette, which also was sent to the London Stock Exchange, British Telecommunications, Lloyds Bank, the Midland Bank, other major banks and manufacturing companies.

"We have never seen anything approaching the magnitude of this attack," said John McAfee, chairman of the Computer Virus Industry Assn., though he noted no damage had yet been reported in the United States. "It took enormous preparation, coordination and a huge amount of money."

People familiar with computer "viruses" and other computer "diseases" were baffled by the maliciousness of the crime, the amount of money and sophistication it required and its lack of any immediately discernible motive.

Computer programs written as pranks or tools of minor sabotage have become ubiquitous over the past few years. But this one was different, according to experts across the country.

The diskette came in a slick package mailed from offices on London's tony New Bond Street. The bright blue cover sheet said the package contained AIDS information, and informed recipients that the information was easy to use and would help them calculate the risks of exposure to the disease.

[This topic seems to be the all-time RISKS record-holder in terms of number of submissions. Most of them were verbatim copies of John McAfee's messages, although John himself did not submit them to RISKS. I was tied up and could not be one of the early harbingers, so at this point I assume almost everyone has heard the story. But just for the record is a summary of it. Those who have been following the story can skip the rest of this issue. PGN]

---

## **Major Trojan Warning**

<portal!cup.portal.com!Alan\_J\_Roberts@SUN.COM>  
Tue, 12 Dec 89 11:26:29 PST

This is an urgent forward from John McAfee:

A distribution diskette from a corporation calling itself PC Cyborg has been widely distributed to major corporations and PC user groups around the world and the diskette contains a highly destructive trojan. The Chase Manhattan Bank and ICL Computers were the first to report problems with the software. All systems that ran the enclosed programs had all data on the hard disks destroyed. Hundreds of systems were affected. Other reports have come in from user groups, small businesses and individuals with similar problems. The professionally prepared documentation that comes with the diskette purports that the software provides a data base of AIDS information. The flyer heading reads - "AIDS Information - An Introductory Diskette". The license agreement on the back of the same flyer reads:

"In case of breach of license, PC Cyborg Corporation reserves the right to use program mechanisms to ensure termination of the use of these programs. These program mechanisms will adversely affect other program applications on microcomputers. You are hereby advised of the most serious consequences of your failure to abide by the terms of this license agreement."

Further in the license is the sentence: "Warning: Do not use these programs unless you are prepared to pay for them".

If the software is installed using the included INSTALL program, the first thing that the program does is print out an invoice for the software. Then, whenever the system is re-booted, or powered down and then re-booted from the hard disk, the system self destructs.

Whoever has perpetrated this monstrosity has gone to a great deal of time, and more expense, and they have clearly perpetrated the largest single targeting of destructive code yet reported. The mailings are professionally done, and the style of the mailing labels indicate the lists were purchased from professional mailing organizations. The estimated costs for printing, diskette, label and mailing is over \$3.00 per package. The volume of reports imply that many

thousands may have been mailed. In addition, the British magazine "PC Business World" has included a copy of the diskette with its most recent publication - another expensive avenue of distribution. The only indication of who the perpetrator(s) may be is the address on the invoice to which they ask that \$378.00 be mailed:

PC Cyborg Corporation  
P.O. Box 871744  
Panama 7, Panama

Needless to say, a check for a registered PC Cyborg Corporation in Panama turned up negative.

An additional note of interest in the license section reads: "PC Cyborg Corporation does not authorize you to distribute or use these programs in the United States of America. If you have any doubt about your willingness or ability to meet the terms of this license agreement or if you are not prepared to pay all amounts due to PC Cyborg Corporation, then do not use these programs".

John McAfee

---

**Re: AIDS DISK UPDATE (I)**

"Kenneth R. van Wyk" <krvw@SEI.CMU.EDU>  
Wed, 13 Dec 89 18:02:50 EST

AIDS INFORMATION DISK  
=====

The latest on this is as follows:

If you have run this disk contact ROBERT WALCZY at PC Business World on 01-831 9252 they have a FREE disk that combats the effects of the disk and they will send a copy to users effected.

Either call Robert or FAX him on 01-405 2347 with your name and address.

The disk should be available in the next day or two.

The program will be available on CONNECT (01-863 6646) for download as soon as it has been tested.

-----

The AIDS disk when installed creates a number of hidden files and directories. You can remove these files by running the program mentioned above or by using the Norton Utilities, PC Tools or equivalent program.

The files that are hidden include a new AUTOEXEC.BAT and a number of other files and directories that contain characters that can not be accessed by standard DOS commands. You will need to rename the files/directories before

they can be deleted.

This information will be updated as we learn more about the disk.

Alan Jay -- The IBM PC User Group -- 01-863 1191.

\*\*\* APPENDED 12/14/89 09:17:07 BY PU/MELINDA \*\*\*

Append on 12/14/89 at 09:17 by Lew Shepherdson, Simware:

I was at a seminar a couple of weeks ago and we had a session on viruses. Some interesting predictions...

1. Benign (non-destructive) viruses will die out...just a passing fad
2. Expect big increase in 'political' viruses...groups spreading vir which promote a political/environmental/human rig and are counting on intense coverage by eager media
3. Expect an increase in 'extortion' viruses aimed at particular vendors... 'If we don't get \_\_\_\_\_, we will release a virus that only attacks your product, etc...'
4. There's a real danger that political hysteria by passing some stupid laws.
5. Expect diskless workstations to be a high-growth mark

Lew Shepherdson  
Simware Inc.

\*\*\* APPENDED 12/14/89 09:17:25 BY SIW/LEW \*\*\*

Append on 12/14/89 at 09:59 by Melinda Varian <BITNET: MAINT@PUCC>:

Received: by PUCC (Mailer R2.06X) id 9330; Thu, 14 Dec 89 07:45:07 EST  
Date: Thu, 14 Dec 89 07:42:06 EST  
Sender: Virus Alert List <VALERT-L@LEHIIBM1>  
Comments: Resent-From: Kenneth R. van Wyk <krvw@SEI.CMU.EDU>  
Comments: Originally-From: Alan Jay <alanj@IBMPCUG.CO.UK>  
From: "Kenneth R. van Wyk" <krvw@SEI.CMU.EDU>  
Subject: Re: AIDS -- UPDATE II -- What can you do.

AIDS INFORMATION DISK

=====

Update 2 13-Dec-1989 6pm

IF you have not run this disk DO NOT INSTALL it appears to be a very cleverly written TROJAN program that can be activated by a number of methods. Currently the activation method that has been detected uses a counter of the number of system reboots. When the counter gets to 90 the system goes into a second phase and encrypts files and directories on your hard disk.

The program appears to have a number of embellishments that makes one think that the front door we have been shown MAY not be the only method that the system uses for deciding when to activate. This is a very nasty program and the only 100% safe thing to do is to backup all DATA files and perform a full reformat of your hard disk.

Followed by a reinstallation of all DATA, from your backup, and programs from original system disks (or backup prior to installing this software).

This should only be attempted once at least TWO copies of all valuable data have been extracted from the system. Please remember to boot your system off an original DOS disk before starting this procedure.

Full details of the suggested procedure will be posted tomorrow.

Alan Jay

Readers who do not wish to follow this route may be interested to in the following information about the primary activation system.

1) A hidden 'ACTOEXEC.BAT' file contains

```
CD \<ALT255>  
REM<ALT255>
```

it then runs your AUTOEXEC.BAT which the program renamed AUTO.BAT

2) A hidden subdirectory <ALT255> contains a file REM<ALT255>.EXE

Each time the system is booted the program is run and the counter incremented/decremented. After 90 activations the system enters phase TWO.

Please note that the system uses the <ALT255> character 'hi space' in the file names to stop standard DOS procedures acting on these files.

IT MAY be possible to delete these entries and thereby disable the program this is NOT certain and it will take several months to discover if this is a safe course of events to take.

I hope that this information helps. I also understand that this is in the hands of the Fraud Squad / Computer Crime Division of the Metropolitan Police. If you have any further information I am sure that they would be interested to here from you.

Alan Jay -- IBM PC User Group - 01-863 1191

\*\*\* APPENDED 12/14/89 09:59:16 BY PU/MELINDA \*\*\*

Append on 12/14/89 at 14:02 by Rich Greenberg, Locus Computer Corp., L.A.:

The AIDS virus was mentioned on the local radio news broadcast as having hit  
The RAND Corp in Santa Monica, Ca.

Rich

\*\*\* APPENDED 12/14/89 14:02:45 BY LCT/RICH.G \*\*\*

Append on 12/15/89 at 00:50 by John Lynn - Mobil Technical Center:

Sick sick sick! AIDS kills on a daily basis, so I guess that makes a 'clever'  
topic to exploit. And \$300+ dollars, plus a 256K minimum memory requirement?!  
For an AIDS questionnaire? Very imaginative...

Guess they got tired of pulling wings off of flies...

-- John (Sorry, but enough is enough, wouldn't you say?) Lynn



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 9: Issue 56

Thursday 21 December 1989

## Contents

- [GAO Says IS technology is transforming the Government](#)  
[Dave Davis](#)
- [California Supreme Court endorses computerized horoscopes](#)  
[Clifford Johnson](#)
- [Software malpractice](#)  
[Steve Philipson](#)
- [Computerized card catalog](#)  
[Roy Smith](#)
- [Frustrated with phones](#)  
[Shamus McBride](#)
- [23 years MTBF ???](#)  
[David A. Honig](#)
- [Re: Another runaway military computing project: WWMCCS](#)  
[Tom Reid](#)
- [Virus Hearing on TV](#)  
[Marc Rotenberg](#)
- [Risks of posting to risks!](#)  
[Joe Dellinger](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **GAO Says IS technology is transforming the Government**

*Dave Davis* <[davis@mwunix.mitre.org](mailto:davis@mwunix.mitre.org)>  
*Thu, 21 Dec 89 07:57:19 EST*

Today's Washington Post (12-21) reports on a General Accounting Office study, "Financial Integrity Act" about Information Technology applications within the government. The overall message is that information systems technology is costly and risky. Here are some quotes:

"Federal agencies operate over 53,000 unclassified automated systems...life cycle costs in the billions of dollars..." The article reports costs of \$17 billion for fiscal 89 versus \$9 billion in fiscal 82 for these computer applications.

"Invariably these systems do not work as planned, have cost overruns in the millions and even hundreds of millions of dollars, and are not developed on time. Congressional interest..has increased..."

Some specific examples are cited.

"...defense [business as well as command and control] far exceeded their original costs estimates...fell significantly short of expectations...design flaws, misjudgments in requirements, poor program management."

The article describes a Navy financial system whose costs grew from \$33 million to \$479 over nine years of development. Also, an IRS system is estimated to cost \$1 billion, and has not shown benefits from currently operational components.

Except for specific details, all of this is old news to many of us who have been involved in large systems of various kinds for a while. What does seem to be new are trends toward larger fiascos and for increased government concern a by people who control purse strings. Also, do stories of such failures indicate that we reach an intellectual brick wall when we try to develop large systems? Or, are we simply repeating dumb mistakes?

David Davis, MITRE Corp., McLean, VA

Standard Disclaimer

---

### **California Supreme Court endorses computerized horoscopes**

*"Clifford Johnson" <GA.CJJ@Forsythe.Stanford.EDU>*

*Tue, 19 Dec 89 15:58:44 PST*

Excerpted from the S.F.Chronicle, 19 Dec 1989:

The California Supreme Court cleared the way yesterday for the use of standardized psychological tests in criminal trials to prove that a defendant does not fit the personality type likely to have committed the charged crime. In a 5-2 ruling, the court rejected a comparison that likened personality tests to lie detectors or voiceprints, which are excluded from trials because their reliability is not commonly accepted by the scientific community. The court majority said introduction of standardized psychological tests in trials is not a revolutionary development and the tests reliability can be challenged by prosecutors.

"We see no reason to subject (these tests) to the special restrictions governing admission of new, novel or experimental scientific techniques not previously accepted by the courts," wrote Justice David Eagleson for the majority.

Chief Justice Malcolm Lucas dissented, saying the decision opened the way for new "mini-trials" focusing not on a defendant's guilt or innocence but on his personality profile and whether it conforms to "the profile displayed by the average child molester, robber, arsonist, or whomever." He acknowledged that personality tests have been admitted by some courts to show a

defendant's mental state at the time of the crime. But that is "far different than using them to exclude defendant from the relevant class of defenders in much the same manner as a blood test or voice print," Lucas wrote.

With the vote, the court reversed the child molestation convictions of a Kern County couple found guilty of committing lewd acts with four young boys in 1983 and 1984. During the trial of Margie Grafton and Timothy Palomo, they attempted to call as an expert witness a psychologist who had given them two commonly used tests -- the Minnesota Multiphasic Personality Inventory and the Millon Clinical Mutiaxial Inventory. The psychologist, Roger Mitchell of Bakersfield, was prepared to testify on the basis of the test results and his interviews with Grafton and Palomo that they showed no indications of deviance and were unlikely to be involved with the charged crimes.

Out of the presence of the jury, Mitchell told the trial court judge that the 566-question Minnesota test, copyrighted in 1943, had a reliability rating of over 70% [sic!!!] in diagnosing the illness of some patients and included hidden questions that detected lies by the person taking the exam.

Many experts believed that the test makes it impossible [sic!!!] to conceal an abnormal personality profile, Mitchell told the judge.

But the trial judge ruled that Mitchell could not testify because the defense had failed to prove the tests met the legal standard of general acceptance in the scientific community.

The court yesterday overturned that ruling, saying the judge should have allowed Mitchell to testify. The majority also found that if his testimony had been allowed, it may have changed the outcome of the case.

What has this to do with comp.risks? The tests at issue are all wholly computerized. Moreover, as if common sense were not enough, it is well established (the tests were statistically debunked in the 1960s) that the maximum accuracy of diagnosis, in most unrealistically favorable circumstances, is of the order of 20% -- hardly an improvement over a guess. Besides, the test is readily foolable, so much so that it is generally regarded as per se invalid the second time it's taken by the same person. Moreover, the "reliability" pertains only to the crudest mental types of disability (schitzophrenia, paranoia, and five other yes/no nasties), whereas the computer tests are generally preprogrammed to spew out pages of rambling mumbo-jumbo analogous to daily horoscopes, except that long psychiatric words are used. Such print-outs more often than not contradict themselves in details.

I was once compelled to take such a test, by a California judge. The examiner, who actually gave classes in psychology to high-power groups of attorneys and judges, without blush permitted me to answer difficult questions by tossing a coin, because I said that was my "natural response" to the test. Still, the computer nevertheless reported that the test was "valid." On one page it reported that a compelling aversion to publicity, on another that I avidly desired publicity. One amusing diagnosis was the computer's finding that I lacked a sense of humor!

I think this is worth the long posting, because these computerized tests are administered almost universally now, and decide everything from employability to the suitability of a mother to be a mother.

---

### ✂ Software malpractice (Jacky, [RISKS-9.52](#))

*Steve Philipson <steve@eos.arc.nasa.gov>*

*Mon, 18 Dec 89 22:30:58 PST*

A few weeks ago there appeared an article in RISKS that reported on a computer software firm that had been successfully sued for "software malpractice". I didn't keep the article, so my details are sketchy. As I recall, the judge found that a programmer was culpable since he did not abide by ACM standards for software, and since he was an ACM member he should have adhered to those standards.

This has been nagging at me for days. I've been an ACM member for some eight years and I've never even SEEN these standards. Furthermore, I do not necessarily endorse ACM standards just because they are from ACM. The industry certainly hasn't embraced all ACM standards (or any one else's for that matter).

Even if one DOES endorse the standards, one wouldn't necessarily use them in all cases. For example, when writing experimental or demonstration software, formal development methods are often not used. The efficacy of the "quick and dirty" approach notwithstanding, there are time when this is done UNDER THE DIRECTION of management AND the customer.

It boggles the mind to consider the possibility that one could be sued for "software malpractice" without there being a formal definition of it or a legal standard. Breach of contract might have been a reasonable finding, but this???? I've heard it said in many arenas that the legal system in this country is out of control. This seems to be yet another example of a system out of kilter. Will this lead to a situation where no one dares to sell software to another party? Will programmers seek to defend themselves from their employers for fear of software quality violations? Stay tuned...

---

### ✂ Computerized card catalog

*Roy Smith <roy@phri.nyu.edu>*

*Sun, 17 Dec 89 23:05:05 EST*

The Brooklyn Public Library has recently put in a computerized card catalog system. The branch nearest me (the main branch, as it turns out) has about 4 terminals in the main lobby, which also contains the card files (in GOK how many thousands of drawers). It hasn't taken people long to become totally dependent on the computerized system. Typically there are lines with 2-4 people waiting at each terminal (probably a 5-20 minute wait) and not a single soul using the card files. Unless there happens to be a terminal free (very rare) I just do it the old fashioned way. I can look up 3 or 4 books in much less time than it would take me to wait for a turn at the terminal. I wonder

how long the average person will wait to use the "new fast computerized catalog" before resorting to the "old slow way", even if the old way is faster.

---

### **✂ Frustrated with phones**

*Shamus McBride <slm%wsc-sun@atc.boeing.com>*

*Mon, 18 Dec 89 15:09:01 PST*

The Bellevue, Washington, Journal American ran an article on telephone glitches collected from its readers.

o "... a dark stormy night, a desperate woman, a telephone from Kafka".

Using a pay phone at a service station along the highway, she dialed 0 then the number and the phone went dead. She tried again and again. She finally reached an operator and found out that (a) the phone was owned by a private company (not AT&T), (b) collect calls could not be made, and (c) she could not be connected with an AT&T operator.

o Another woman received hourly calls with the recorded message

"The maximum dollar amount is exceeded by the number 4-4-4-4-4-4."

The problem was traced to a pay phone at a local gas station with a full coin box. The phone was programmed to call someone when the coin box was full. Unfortunately, it was programmed with the wrong number.

o For six months a woman had long distance calls to Mexico City on her bill. The phone company finally discovered that the woman's line was cross wired with a neighbor's line. The twist in the story was that the neighbor had recently moved into the house and did not realize it had TWO lines (the phone company had failed to disconnect the second line when the previous owner moved out). The neighbor's bill looked normal since most of his calls were on his primary line. Only when he used a secondary phone were the calls billed elsewhere.

o One family had phones that rang three times then stopped.

Friends said they called and let the phone ring 20 times and no one answered. "After extensive investigation [GTE] found an electronic glitch at a nearby central office."

The article concluded: "the letters we received showed that people are dependent on the telephone and, when things go wrong, hardly in a mood to hear a pitch about the values of consumerism. True phones don't go wrong often, they said, But when they do ..."

---

### **✂ 23 years MTBF ???**

*"David A. Honig" <honig@BONNIE.ICS.UCI.EDU>*

*Fri, 15 Dec 89 11:47:08 -0800*

In the recent Electronic Design News (a trade newspaper), the cover story is about Fujitsu's recent claims of 200,000 hrs MTBF on some of its hard drives. That is nearly 23 years of 24-hour continuous use. Needless to say, this number is not obtained from units in the field, but extrapolated from their test data. Other manufacturers consider that number to be marketing strategy, although some have large (but not that large) numbers, too. If its any consolation, the article said that the drives had a 5 year warantee...

I could not help but be reminded of the  $10^{-9}$  claims of some software producers...

---

**✂ Re: Another runaway military computing project: WWMCCS**

*Tom Reid x4505 <reid@ctc.contel.com>*

*Fri, 8 Dec 89 14:22:05 EST*

I worked with WWMCCS in 1985/6 and many of their problems stemmed from a technology bet that they had made 3-4 years earlier. They had a software first philosophy that stressed using as much commercial-off-the-shelf (COTS) software as possible. They bet that by 1986, respondents to the RFP would be able to bid COTS 1) multi-level secure operating systems and 2) distributed heterogeneous DBMSs. It is 1989 and there are still precious few (if any) examples of either. When it became obvious that neither was going to appear by 1985/6 when they were scheduled publish the RFP, they were not prepared and the program began scrambling to find stop gaps. It was downhill from there.

---

**✂ Virus Hearing on TV (CPSR, too)**

*<mrotenberg@cdp.uucp>*

*Fri, 15 Dec 89 12:38:30 -0800*

The November House Judiciary Committee hearing on computer virus legislation will be shown on C-Span on December 23 (8:45 am) and December 24 (1:30 am). This was an interesting and timely event with representatives from NIST, ADAPSO, CBEMA, CPSR, and members of Congress discussing technical and legal responses to the issues raised by computer viruses.

The prepared CPSR statement on computer virus legislation is available from the CPSR Washington office. Please send me a note if you would like a copy.

Marc Rotenberg.

---

**✂ Risks of posting to risks!**

*Joe Dellinger <joe@hanauma.stanford.edu>*

*Tue, 19 Dec 89 21:37:01 PST*

In the last few days I have learned the risks of posting to comp.risks!

1) No, Convex's "lint" does not edit files, I meant "indent"! Oops.

(Re: Fun and Games with Indent, [RISKS-9.54](#))

2) I also learned the dangers of using questionable terms like "yellow peril". I thought these days that "yellow peril" was so outdated that it carried about the same force as "Redcoats". Evidently I was wrong. If I upset anybody, I'm sorry. You can stop educating me as to the correct current popular definition now! Hopefully in a few decades or so my usage will become correct.

(Re: Risks of Mail, [RISKS-9.55](#))



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

**Volume 9: Issue 57**

**Thursday 4 January 1990**

## Contents

- [Self-Service ordering in retail establishments](#)  
[Russell McFatter](#)
- [Programming Languages and Romanian Dictators](#)  
[Eric Haines](#)
- [`Credit Card' found from 13th Century](#)  
[Steve Crocker](#)
- [Risks of computerfax](#)  
[Steve Elias](#)
- [Password Security: A Case History, by Bob Morris and Ken Thompson](#)  
[PGN](#)
- ["What Really Happened Oct. 13"](#)  
[Joe Morris](#)
- [The risks of not learning?](#)  
[Al Arsenault](#)
- [RAND has not received "AIDS Information Disk"](#)  
[Correction from Jim Gillogly](#)
- [Call for Papers -- 13th National Computer Security Conference](#)  
[Jack Holleran](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✉ Self-Service ordering in retail establishments

*Russell McFatter <[russ@GARP.MIT.EDU](mailto:russ@GARP.MIT.EDU)>  
Fri, 22 Dec 89 17:34:13 est*

In [RISKS Digest 9.56](#), Roy Smith talks about delays waiting for computerized card catalogs (and that it was sometimes faster to use the old-fashioned approach).

I find that one of the best advantages of electronic self-service is that it usually provides FASTER service than waiting for a human operator; A good example is bank ATM's. (I can usually park my car, go inside the bank, transact my business, and be back in the car and on my way before the FIRST car in the drive-thru line has left).

Usually, the speed-up advantage for these cases is offset by a loss in convenience. Two examples:

(1) Most Service Merchandise catalog showrooms in the area have one or more "Silent Sam" self-service ordering stations. These are (basically) dumb terminals which can collect your name and address, take orders, and will even tell you if a particular item is out of stock or that only the "display" item remains. (Amazingly, the inventory counts seem to be reasonably accurate!). However, the station does not print a receipt; the receipt gives you, at least, the "guaranteed" time that your order will be filled by. Without the receipt, you have no idea how long you'll be waiting, and if the order is delayed or forgotten, you have nothing with which to claim the "reward" usually offered for these cases.

(2) Burger King is experimenting with a self-service ordering system called "Touch and Go": an ATM-like device with the complete Burger King menu on a large touchpad display. Posters and a nearby video player encourage customers to "avoid long lines" and use the "simple" Touch-and-Go system. The machine takes your order, takes your money, and gives you a change and your receipt; you then proceed to the "Touch and Go" area at the counter to pick up the food. (It even takes/gives pennies!!)

When I first tried this at the Acton store, I was impressed at the smarts (if you order a "breakfast" item at dinnertime, for example, a voice and CRT display both tell you that "this restaurant is not serving breakfast at this time"). Then I tried to order a double cheeseburger with "ketchup only"; and found it impossible. I mentioned this to one of the employees while placing my MANUAL order, and was told that the software was going to be upgraded shortly to allow special orders. The machine was the only one of its kind and was being market-tested in the Acton, MA store.

A few weeks go by, and sure enough, an extra option is added to let you customize individual items. So I order the double cheeseburger again, and press the "Have It Your Way" button. New options appear on the CRT: "Adjust Ketchup" and "Adjust Pickle". Both are set to "normal", so I touch "Adjust Pickle" and set "Pickle" to "None". Great, an electronically-ordered "ketchup only" double cheeseburger at last!

What do I actually get? A double cheeseburger with ketchup and mustard. Seems that mustard is normal on a double cheeseburger, and Touch-and-Go offers no way to turn it off. I bring the burger up to the counter where they acknowledge this, and replace the cheeseburger for free. "I'm glad you brought it back," the salesperson tells me. "This has been happening a lot. The machine goes on the road next week; we'll be glad to be rid of it."

--- Russ McFatter [russ@alliant.Alliant.COM]

"Have It Your Way" and "Touch-and-Go" are (undoubtedly) trademarks of Burger King Corporation, for what it's worth. Std. disclaimer applies.

## ✂ Programming Languages and Romanian Dictators

Eric Haines <erich@eye.UUCP>

Fri, 29 Dec 89 08:50:32 est

This somewhat cryptic paragraph is from "Romanians Talk of Life Then and Now" by Russell W. Baker, in the Christian Science Monitor, December 27th, 1989:

Dragos Vaida, an associate professor of mathematics at the University of Bucharest, told how he had published a book on computer science, but was obligated to change the title because it referred to programming languages. Elena Ceausescu, who was in charge of technology, was against computer science, he said, because it gave the people technical knowledge that could be used against the dictatorship.

What I'm curious about is what the new unoffensive title could have been. If Elena was upset about computer science in general, why wasn't the book simply banned? Or was she upset that people might learn about "programming languages", which to her might sound like mind control? Strange story.

Eric Haines - wrath.cs.cornell.edu!eye!erich

---

## ✂ `Credit Card' found from 13th Century

<crocker@TIS.COM>

Wed, 27 Dec 89 16:47:49 -0500

The last paragraph suggests the RISKS were the same 700 years ago.

[From The Times (London) Saturday, December 23, 1989 by Simon Tait, Arts Correspondent]

A seal, which would have been the equivalent of cheque card, passport and credit card rolled into one for the person who lost it more than 700 years ago, has been found by archaeologists working in Oxford.

Mr. David Dawson, of the Oxfordshire County Museum, Woodstock, where the seal will go on display, said: "This was a personal seal which would have been carried round everywhere by the owner. He would have been lost without it, and it is a rare thing to find because it would normally have been destroyed on his death."

What makes the small, corroded and fragile 13th-century seal unique is that it was found in premises known, through records in the Bodleian Library, to belong to the seal's owner.

It bears the legend `S' ROGERUM COMENORE CLICI, indicating that the seal (sigillum) belonged to Roger of Cumnor, clerk or priest, who worked as a lawyer. The site is on the corner of Hollybush Row in Oxford, on which Halls Brewery stood most recently, which is being developed by Grosvenor Square Property Developers.

Roger who gave two buildings on it to Oseney Abbey in 1265, during the reign of Henry III, according to the Bodleian Library. The seal was found in a ditch between the two buildings.

Mr. Brian Durham, a member of the Oxford Archaeological Unit which made the discovery during excavations last week, said: "The new find could be a forgery but the more likely explanation is that it is his early seal, which he lost when he was actually living in the house. You can picture him hunting unsuccessfully for it."

"Since he worked, in effect, as a solicitor, he would have had to alert everyone to the fact that the seal could have been stolen and used for forgeries. Then he would have had to have a different seal made."

---

### ✂ Risks of computerfax

<eli@pws.bull.com>

Fri, 29 Dec 89 09:25:15 -0500

Commercial email to fax gateways are beginning to hit the market. I've been faxing email for people for many months, and one problem which recurs is people supplying me with incorrect fax numbers. I usually try a voice call first, to ensure that the destination phone number is indeed answered by a fax machine. Occasionally it is not, and I am forced to confuse the innocent person who answers. Often, the person can supply me with the correct fax number.

This problem is compounded with fully automated computerfax systems. Some computerfax hardware is able to detect voice on the line, and hence "do the right thing": don't call again, and return an error. Some computerfax systems do not properly detect voice, and they might redial the phone number N times before returning an error.

One solution might be to use computerfax hardware that has the capability to play digitized voice and ask the recipient to press touch tones to indicate his annoyance level! Most computerfax hardware does not have this capability, unfortunately.

A risk is that blue network meanies would purposely ask for a fax to be delivered to a non-fax number, in order to cause an "annoyance". Annoyance calls are illegal. I wonder whether the computerfax machine owner is liable for such calls, or whether the sender is responsible? (comp.dcom.telecom cats can probably answer this question.)

We've seen the uproar in Washington about junk faxes... Computerfax opens the door for an email user to cause junk fax, intentionally or unintentionally.

Steve Elias 508 671 7556

---

### ✂ Password Security: A Case History (Bob Morris and Ken Thompson)

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

Wed, 3 Jan 1990 16:21:49 PST

I just happened to be rereading the above cited paper (CACM, 22 11, Nov 1979, pp. 594-7), and stumbled upon Bob Morris' tale about discovering the password file spewing out instead of the message of the day file on each new login, because two people were editing the two files in the same directory and the editor used the same temporary file names for both of them (MIT's CTSS, early 1960s). Yes, it really happened. But since this case is often cited as a piece of apocrypha, I thought it might be worth mentioning here, particularly for the younger folks for whom 1979 (not to mention the early 1960s) is prehistory.

[That is the paper that describes preencryptive attacks on the encrypted password file.]

---

### **✶ A little (much-needed) humor [ WHAT REALLY HAPPENED OCT. 13 ]**

Joe Morris (jcmorris@mitre.org) <jcmorris@mwunix.mitre.org>

Wed, 03 Jan 90 11:29:01 EST

The following appeared in yesterday's (1/2/90) Wall Street Journal in a summary of some of the more absurd events of the past year. The sad part of it is that too many people might take the story as literal truth...while others ignore questions of security as unnecessary makework.

WHAT REALLY HAPPENED OCT. 13:

Arthur Cashin, a Paine Webber trader at the New York Stock Exchange, writes a daily market letter with a touch of the wacky.

The Monday after the Friday-the-13th plunge, when traders were still wondering if the market would crash again, Mr. Cashin explained what really happened Friday:

"At about 2:25 (EDT) a nine-year-old named Lance, sitting hunched over his Nintendo machine in Hohokus, N. J., opened the wrong door in a game of "Mario Brothers." Once the door was open the computer virus escaped and immediately began calling in sell orders to the New York Stock Exchange's DOT system. The virus was programmed to enter the orders in alphabetical order based on industry, so it began with airlines and ended with the zoysia grass distributors (which were least affected by the sell-off)."

"Is that what happened? Well, no! But that is what you will probably hear from a variety of academics and self-appointed experts as regulators review Friday's events."

---

### **✶ The risks of not learning?**

Al Arsenault <AArsenault@DOCKMASTER.NCSC.MIL>

Wed, 3 Jan 90 07:58 EST

During the Fall 1989 semester, I taught a computer security class at a local college. Most of the students were junior or senior CS majors.

One of the questions on the final exam was "Describe one advantage that passwords have over biometric devices (e.g., retinal scanners, fingerprint readers) as an authentication mechanism."

I was expecting answers along the lines of 'passwords are more acceptable to users in most cases than sticking their eyes up to a slot', since I had spent a lot of time covering Saltzer and Schroeder's eight design principles, one of which is 'psychological acceptability' of mechanisms to users. (Other acceptable answers existed - e.g., with biometrics, one must deal with both false positives and false negatives - there's a chance the real person will be rejected.)

One student's answer: "Passwords have the advantage that it's easier to let my friend use my account. If the system uses biometric devices for user authentication, I have to be there when he logs in, to get him on to the system. But, if the system uses passwords, I can just tell him my password, and don't have to be there - he can login at his leisure."

So much for that one-week unit on 'Individual Accountability'.

Al Arsenault

---

### **✂ RAND has not received "AIDS Information Disk"**

*Jim Gillogly <jim%blaise@rand.org>*

*Tue, 19 Dec 89 16:12:39 PST*

In [RISKS 9.55](#) it was reported that a local radio news broadcast said that RAND had been hit with the AIDS virus [sic]. This is not correct. We have not seen the "AIDS Information Disk" here. There was a flurry of activity from the press when AP reported that we had warned our researchers to be on the lookout for the Disk in their incoming mail (true). I talked to several TV stations, passing on the information that it's not infectious (i.e. isn't a virus), and that it underlines the fact that everybody should make frequent backups and be careful what they stick into their computers.

Jim Gillogly

[Also noted by Jim Guyton, guyton@rand.org]

---

### **✂ Call for Papers --- 13th National Computer Security Conference**

*Jack Holleran <Holleran@DOCKMASTER.NCSC.MIL>*

*Sat, 23 Dec 89 08:59 EST*

CALL FOR PAPERS:

13th NATIONAL COMPUTER SECURITY CONFERENCE

Sponsored by the National Computer Security Center and  
the National Institute of Standards and Technology

Theme: Information Systems Security: Standards - The Key to the Future

Date: OCTOBER 1-4, 1990

Location: WASHINGTON, D.C.

This conference provides a forum for the Government and the private sector to share current information that is useful and of general interest to the conference participants on technologies, present and future, that are designed to meet the ever-growing challenge of telecommunications and automated information systems security. The conference will offer multiple tracks for the needs of users, vendors, and the research and development communities. The focus of the conference will be on: Systems Application Guidance, Awareness, Training, and Education, Ethics and Issues, Evaluation and Certification, Innovations and New Products, Management and Administration, and Disaster Prevention and Recovery. We encourage submission of papers on the following topics of high interest:

#### Systems Application Guidance

- Access Control Strategies
- Achieving Network Security
- Building on Trusted Computing Bases
- Integrating INFOSEC into Systems
- Preparing Security Plans
- Secure Architectures
- Securing Heterogeneous Networks
- Small Systems Security

#### Innovations and New Products

- Approved/Endorsed Products
- Audit Reduction Tools and Techniques
- Biometric Authentication
- Data Base Security
- Personal Identification and Authentication
- Smart Card Applications
- Tools and Technology

#### Awareness, Training and Education

- Building Security Awareness
- CompuSec Training: Curricula, Effectiveness, Media
- Curriculum for Differing Levels of Users
- Keeping Security In Step With Technology
- Policies, Standards, and Guidelines
- Understanding the Threat

#### Evaluation and Certification

- Assurance and Analytic Techniques
- Conducting Security Evaluations
- Covert Channel Analysis
- Experiences in Applying Verification
- Formal Policy Models
- Techniques

#### Management and Administration

- Accrediting Information Systems and Networks
- Defining and Specifying Computer Security Requirements

- Life Cycle Management
- Managing Risk
- Role of Standards
- Security Requirements

#### Disaster Prevention and Recovery

- Assurance of Service
- Computer Viruses
- Contingency Planning
- Disaster Recovery
- Malicious Code
- Survivability

#### Ethics and Issues

- Computer Abuse/Misuse
- Ethics in the Workplace
- Individual Rights
- Laws
- Relationship of Ethics to Technology
- Standards of Ethics in Information Technology

BY FEBRUARY 16, 1990: Send eight copies of your draft paper\* or panel suggestions to one of the following addresses. Include the topical category of your submission, author name(s), address, and telephone number on the cover sheet only.

1. FOR PAPERS SENT VIA      National Computer Security Conference  
U.S. or Foreign      ATTN: NCS Conference Secretary  
Government MAIL      National Computer Security Center  
ONLY:      Fort George G. Meade, MD 20755-6000
  
2. FOR PAPERS SENT VIA      National Computer Security Conference  
COMMERCIAL COURIER      c/o NCS Conference Secretary  
SERVICES (e.g.-FEDERAL      National Computer Security Center  
EXPRESS, EMERY, UPS,      911 Elkridge Landing Road  
etc.):      Linthicum, MD 21090
  
3. FOR Electronic Mail: NCS\_Conference@DOCKMASTER.NCSC.MIL (1 copy)

BY MAY 4, 1990: Speakers selected to participate in the conference will be notified.

BY JUNE 22, 1990: Final, camera-ready papers are due.

\* Government employees or those under Government sponsorship must so identify their papers.

For additional information on submissions, please call (301) 850-0272.

To assist the Technical Review Committee, the following is required for all submissions:

Page 1: Title of paper or submission  
Topical Category & keywords  
Author(s)  
Organization(s)  
Phone number(s)  
Net address(es), if available  
Point of Contact

Additionally, submissions sponsored by the U.S. Government must provide the following information:

U.S. Government Program Sponsor or Procuring Element  
Contract number (if applicable)  
U.S. Government Publication Release Authority  
(Note: Responsibility for U.S. Government  
pre-publication review lies with the author(s).)

Page 2: Title of the paper or submission  
-last abstract  
The paper (Suggested length: 6 pages, double columns)

A Technical Review Committee, composed of U.S. Government and Industry Computer Security experts, will referee submissions only for technical merit for publication and presentation at the National Computer Security (NCS) Conference. No classified submissions will be accepted for review.

Papers drafted as part of the author's official U.S. Government duties may not be subject to copyright. Papers submitted that are subject to copyright must be accompanied by a written assignment to the NCS Conference Committee or written authorization to publish and release the paper at the Committee's discretion. Papers selected for presentation at the NCS Conference requiring U.S. Government pre-publication review must include, with the submission of the final paper no later than June 22, 1990 to the committee, a written release from the U.S. Government Department or Agency responsible for pre-publication review. Failure to comply may result in rescinding selection for publication and for presentation at the 13th NCS Conference.

Technical questions can be addressed to the NCS Conference Committee through the following means:

Phone: (301) 850-0CSC [0272]

Electronic Mail: NCS\_Conference@DOCKMASTER.NCSC.MIL

Government Mail: National Computer Security Conference  
National Computer Security Center  
Fort George G. Meade, MD 20755-6000

Commercial Carriers: National Computer Security Conference  
c/o NCS Conference Secretary  
National Computer Security Center  
911 Elkridge Landing Road  
Linthicum, MD 21090



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

**Volume 9: Issue 58**

**Tuesday 9 January 1990**

## Contents

- [New-Years' Lotto goes Blotto](#)  
[Jim Anderson](#)
- [Railroad interlocking systems](#)  
[Douglas W. Jones](#)
- [Sorry, the bank's already debited your mortgage](#)  
[Dave Horsfall](#)
- [Positive fingerprint identification?](#)  
[Dave Horsfall](#)
- [Re: Password Security: A Case History](#)  
[Fernando J. Corbato](#)
- [The risks of not learning - and of ignoring realities](#)  
[Jerry Leichter](#)
- [6th Chaos Communication Congress, Hamburg 27-29 Dec 1989](#)  
[Klaus Brunnstein](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✂ **New-Years' Lotto goes Blotto**

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

Mon, 8 Jan 1990 11:40:31 PST

The Pennsylvania Wild Card Lotto computer systems had to be reprogrammed to accommodate the end of the decade. That had already supposedly been accomplished -- but apparently not carefully enough. In the first Lotto of the new decade, the computer systems were unable to determine the winners and further software fixes were required. [Philadelphia Inquirer, 4 Jan 1990, contributed by James P. Anderson]

---

### ✂ **Railroad interlocking systems**

Douglas W. Jones <[jones@pyrite.cs.uiowa.edu](mailto:jones@pyrite.cs.uiowa.edu)>

Fri, 5 Jan 90 09:49:21 CST

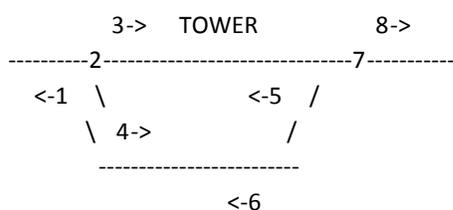
Most of the arguments about safety critical hardware and software that I've seen assume that digital computers pose new problems. In effect, the argument is that safety critical digital control systems are a radical novelty (to borrow from Dijkstra's essay on the Cruelty of Teaching Computer Programming), and thus that they cannot be discussed by analogy to older solutions to the same problem.

One historical parallel which may prove interesting in this context is the railroad interlocking machine. Interlocking machines were purely mechanical digital computing machines that served to enforce a set of operating rules on railroad signalmen operating the switch-tracks and signals at a railroad interchange.

I suspect that there are useful parallels between the history of railroad interlocking machines and the more recent developments in safety critical digital control systems. An error in the logical design of an interlocking machine could easily go undetected until it caused a train wreck, and I wonder if old cases involving railroad interlocking machines might provide useful precedents for many of the software liability questions that have been raised recently.

Here's a short description of the problem solved by a relatively simple interlocking machine:

Consider the following track layout:



1, 5 and 6 are signals controlling traffic from the left.  
 3, 4 and 8 are signals controlling traffic from the right.  
 2 and 7 are switch tracks.

All signals may be up (go) or down (stop).

All switch tracks may be set to direct traffic up to the straight through track or down to the siding.

The control levers for all of the signals and the switch tracks are located in the tower, where the signalman may work them one at a time. (One at a time because it takes his full strength to overcome the friction of the system of cranks and push-rods that connects each lever to the corresponding switch-track or signal.)

The problem: There are 8 levers in a row, each with 2 settings; thus, there are 256 possible states of the system. (I've seen photos of old railroad control towers with banks of 20 or more control levers.) Of these 256 states, only a few are safe.

Example: If switch 2 is set up, switch 7 is set down, and signals 1, 4, 5, and 8 are up, a train entering the

diagram from either side will proceed through the diagram and derail as it passes through the incorrectly set switch at the opposite side of the diagram.

The classic solution: A mechanical interlocking machine is added to the tower. A tower containing an interlocking machine was a sufficient improvement over an un-interlocked control tower that the term interlocking tower came to be applied to such a tower. An interlocking machine consists of a set of 8 transverse rods crossing 8 rods linked to the control levers. Each transverse rod is linked to one of the control rods and at each point where a transverse rod and a control rod cross, the transverse rod may be notched to allow the control rod to move or un-notched to lock the setting of the control rod.

In the above example, signals 1, 3 and 4 would be interlocked with switch track 2 such that the setting of 2 could only be changed if 1, 3 and 4 were in the down position, and so that 3 could only be raised to the up position if switch 2 was set up, and 4 could only be raised to the up position if switch 2 was set down. A similar set of interlocking rules would apply to 5, 6, 7 and 8.

The "program" for the interlocking machine can be viewed as the pattern of notches in the transverse rods.

Modern solutions to the interlocking problem use electrically operated switches and signals with relays and more recently computerized controls to interlock their operation. Long before such modern solutions came into use, interlocking machines were built into the control towers along most mainline trackage in North America. The interlocking machines for simple passing sidings such as I've described above could be standardized, but there were (and are) many places where the track layout controlled by an interlocking tower was unique and required what we would now call custom programming.

Incidentally, in addition to the possible relevance of the history of interlocking towers to modern problems in safety-critical computing systems, lots of good assignments can be derived from this problem. For example, given a set of interlocking rules, derive a finite-state machine describing the legal states transitions. Alternately, write a program that, when given the current state and a (partial?) specification of a desired state, produces a plan for a series of legal transitions that will reach the desired state.

Douglas Jones, Dept. of Computer Science, Univ. of Iowa, Iowa City, Iowa, 52242

---

### **✂ Sorry, the bank's already debited your mortgage**

*Dave Horsfall <dave@stcns3.stc.oz.au>*

*Sat, 6 Jan 90 22:49:18 est*

In the wake of sky-rocketing mortgage rates in Australia comes this story from the "Sydney Morning Herald", Friday January 5th, 1990:

``Sorry, the bank's already debited your mortgage

As many as 100,000 Commonwealth Bank customers found their accounts prematurely depleted yesterday when a computer debited home loan payments due for any day in January rather than just Wednesday.

The Commonwealth's general manager, retail, Mr Peter Andrews, said staff became aware of the mistake when some customers found cheque or Keycard accounts debited ahead of time.

Mr Andrews said a computer sweep on Tuesday night would normally have debited customers who had elected to pay their home loans automatically on Wednesday.

The error affected up to 100,000 home loan holders throughout Australia, but Mr Andrews said most customers would not have become aware of it. They would have noticed "only if they were taking money out and found their accounts were overdrawn," he said. Emergency arrangements had been set up to give them access to cash."

Dave Horsfall (VK2KFU), Alcatel STC Australia, dave@stcns3.stc.oz.AU  
dave%stcns3.stc.oz.AU@uunet.UU.NET, ...muninari!stcns3.stc.oz.AU!dave

---

### **✂ Positive fingerprint identification?**

*Dave Horsfall <dave@stcns3.stc.oz.au>  
Mon, 8 Jan 90 19:28:21 est*

The following is taken from "The Sydney Morning Herald" Mon 8th January:

``Positive identification

It might not have caught the killer, but at least it has identified the victim. A fingerprint checking computer immediately revealed to Seattle police the identity of a body found along a busy road in Portland. A manual fingerprint comparison, using the police department's hundreds of thousands of fingerprint files, would have taken months, according to police. The computer's positive identification [ emphasis mine ] took just a few seconds."

Dave Horsfall (VK2KFU), Alcatel STC Australia, dave@stcns3.stc.oz.AU  
dave%stcns3.stc.oz.AU@uunet.UU.NET, ...muninari!stcns3.stc.oz.AU!dave

---

### **✂ Re: Password Security: A Case History**

*"Fernando J. Corbato" <corbato@LCS.MIT.EDU>  
Mon, 8 Jan 1990 18:02:43 EST*

Peter's note recalling the colossal time-sharing mishap of the interchange of the message-of-the-day with the password file which occurred on CTSS in the

early 1960's made me go look up the article and see what was said about the cause. The article says "due to a software design error, the temporary editor files of the two users were interchanged..." but it was deeper than that.

To simplify the organization of the initial CTSS system, a design decision had been made to have each user at a terminal associated with his own directory of files. Moreover the system itself was organized as a kind of quasi user with its own directory which included a large number of supporting applications and files including the message-of-the day and the password file. So far, so good. Normally a single system programmer could login to the system directory and make any necessary changes. But the number of system programmers had grown to about a dozen in number, and, further, the system by then was being operated almost continuously so that the need to do live maintenance of the system files became essential. Not surprisingly, the system programmers saw the one-user-to-a-directory restriction as a big bottleneck for them. They thereupon proceeded to cajole me into letting the system directory be an exception "since system programmer's would be careful to not make mistakes."

But of course a mistake was made. Overlooked was that a software design decision had been made in the standard system text editor that it would only be used by one user at a time working in one directory so that a temporary file could have the same name for all instantiations of the editor. And with two system programmers editing at the same time in the system directory, the disaster of the swapped temporary files finally occurred.

The tale has at least two morals: First, design bugs are often subtle and occur by evolution with early assumptions being forgotten as new features or uses are added to systems; Second, even system programmers make mistakes so that prudent system management must be based on expecting errors and not on perfection.

F. J. Corbato

[For our younger readers, Corby was the father of both CTSS and Multics. PGN]

---

### **✂ The risks of not learning - and of ignoring realities**

*<Leichter-Jerry@CS.YALE.EDU>*

*Fri, 5 Jan 90 12:45 EST*

In a recent RISKS, Al Arsenault records his distress at an answer he received on a test he gave in a course on computer security. A student stated that one advantage of passwords over biometric authentication was that he could give his password to a friend so that the friend could use his account. Mr. Arsenault comments, "So much for that one-week unit on 'Individual Accountability'".

I'm afraid he is missing an important point. The fact of the matter is, people lend things to friends. They lend clothes, they lend cars, they lend money. They let people use their telephones. They even lend things like ID cards when they can get away with it. Those in charge of things like security cards don't like this, and they try hard to prevent it, resulting in a continuous battle with people who just want to continue to live their lives.

At times, it's easy to forget that most people share neither the world view nor the interests of the "security community". Yes, they are aware that they should not let "anyone" know their bank card password - but when, for example, they are sick in bed they consider it a useful thing that they can give the card and password to a friend and have him get some money and do a bit of shopping for them. This, too, is a positive good.

I'm sure Mr. Arsenault covered the standard set of distinctions among identification schemes - something you KNOW, something you HAVE, something you ARE. Each has its own features, which in different contexts may be good or bad. Something you KNOW can be replicated to others; something you HAVE can be lent; something you ARE can't be transferred. These are neither advantages nor disadvantages; they are simply inherent features.

Consider an analogy: Why is letting someone use your computer account inherently different from letting someone use your telephone? Would you never be willing to tell a trusted friend your telephone access code?

-- Jerry

[Yes, some people are concerned about computer security and others are not -- at least not until they've been burned. But Reality and Sensibility are in this case two radically different things. If you want individual accountability, you do not share passwords. The telephone system is intrinsically vulnerable to illicit use of credit cards. If you wish to trust a friend, that may have low risk -- unless MANY people are involved; then you might like to have records that show who is actually using your resources. However, suppose you are designing a computer system that recognizes fingerprints as authenticators. It would be rather silly to design the system to recognize facsimile copies of a fingerprint so that someone else could conveniently enter the system when provided with a fingercopy (which can itself be repeatedly copied). (Ignore the fact that the previous person's fingerprint may be liftable from the glass!) Much more sensible is to design the computer system so that it encourages individual accountability, while also permitting flexible controlled sharing. That is what Multics was all about in 1965. What's new? PGN]

---

## ✶ 6th Chaos Communication Congress, Hamburg 27-29 Dec 1989

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

*05 Jan 90 14:41 GMT+0100*

6th Chaos Communication Congress 1989

'Open frontiers: CoComed together'

The 6th annual congress of Hamburg's Chaos Computer Club (CCC) was held on 27-29 December 1989 in Hamburg. The recent political development in Germany also influences the hacker scene; only after a controversial debate, the organisers denied a suggestion to move the congress to East Berlin. Among the about 300 visitors, about 50 people from East Germany were present. A few foreign visitors came from France, Netherlands and USA. The congress was male-dominated, with a growing female participation (about 40). The other major German hacker groups (from Bavaria, Cologne) were not present.

Following trends of the 5th CCC congress, themes relating to computer security were less dominant. As CCC members and congress organisers age and their professional background dominates (a significant part works in computing), the political impact of computerisation becomes dominant, not only under a revised West/East German scenario. Even the presentation of comp.security changes: invited speakers with solid scientific background lecture in traditional style, some even with overhead folios from international conferences; even a state attorney (responsible for the case FRG vs.S. Wernery re hacking!) participated in a surprisingly fair and open discussion on criminal law against hacking.

Major themes were:

- information about computerisation and network infrastructure in East Germany
- cooperation with East German computer freaks
- cooperation with eco-groups
- 'female computer handling'
- KGB-hacker 'Hagbard'
- Security in open networks (2 invited speakers)
- Hacker Ethics and Harper's Hacker Conference (Capt.Crunch)
- Free Flow of Information, Copyright
- UNIX discussions: several workshops, UUCP
- Virus Forum II.

Several sessions were devoted to the state and possible developments of computers + communication (c+c) in East Germany. With insufficient computers and an outmoded telephone net, CCC appealed to the German public to donate unused equipment (C64, Apple II, PCs) to eastern groups. As substitute of the insufficient telephone net, the recently installed 'packet radio' should be used for computer communication; pc-communication with packer-radio was demonstrated at the exhibition. As a start of computerisation, CCC plans to hold another congress (Kaos Kommunikation Kongress) in East Berlin early in 1990.

Representatives of the East German citizen movement, esp.from 'New Forum' discussed possible developments. Many participants (most oriented towards the left wing of the political spectrum) advised the East Germans not willingly to follow West German c+c industry and public authorities (Telekom) to install traditional technology; as an example, ISDN is widely criticized because it neglects data protection laws.

Following discussions on CCC congress 88, several projects of ecological data processing and communication started (e.g. data collection in the environment of industry and nuclear power plants). CCC and some eco-groups plan to install an information center on a ship during the EEC's North Sea conference (March 1990). A special session and workshop was also devoted to female computer-handling; a group of male (30) and female (20) participants discussed the role and attitudes of women in education and profession; similar discussions in national and international conferences (e.g. IFIP TC-9) may point to revised design principles (e.g. reduced complexity, possible plausibility control).

Only a minor part of the congress was devoted to traditional hacker themes. Surprisingly, CCC did not follow it's tradition to extensively discuss hacker

experiences of the last year. The KGB hack (broadly published in March, 1989) was \*no theme\*; instead, a session was devoted to the memory of Karl Koch alias 'Captain Hagbard', one of Cliff Stoll's 'Wily Hackers' (CACM 5/1988) who, after having informed the public authorities as one of 2 chief witnesses in the case, committed suicide. 3 personal friends (without any interest in computing) and PENG0 (the other chief witness) described Hagbard's sad life story, full of family problems and addictions (drug, hacking). The role of the media as well as CCC's role (part of which had strongly denied any contact to the crackers) was controversially discussed.

Btw: the trial against 3 KGB hackers will begin on January 11,1990.

A whole 4 hour session was devoted to 'Security in open networks', with Dr. Raubold (director in GMD, the national research institute for computers and communication) and Dr. Pfitzmann (Karlsruhe, Faculty for Informatics) introducing into technologies of encryption (DES, RSA) and of secure communication in open networks; the 20 participants which stayed until the end were mainly students of Informatics and programmers.

'Captain Crunch' reported about the recent electronic conference which was sponsored by Harper's; the results will be published in this magazine early in 1990 (survey document in English available on request). He moreover demonstrated, via AT+T operator switched connection, PicturePhone.

Virus Forum II (1989) was intended to show the developments since Forum I (1985) where CCC made viruses publicly known in FRG. Ralf Burger (author of a Virus Book, where he published also virus code including a MVS/370 virus), Wau Holland (CCC's founding father), Juergen Wieckmann (editor of Chaos Computer Book) and K.Brunnstein discussed trends of viruses. Meanwhile, more than 80 viruses are known on INTEL 80xxx-systems, and more than 70 on several 68.000-systems as AMIGA, Atari and MacIntosh. Viruses are found to grow from 'families', the descendants of which are ever more difficult to analyse and produce growing damages.

While the participants agreed in the threat assessment, there was significant disagreement about the consequences. Burger argued that everybody can program a virus; publication of virus code does not contribute to the virus threat.

Brunnstein argued strongly against, that many young programmers learn to program viruses mainly from published code which they change slightly to produce their own virus; even if they program a virus for learning purposes, they loose control when it spreads via the friends' diskettes. Virus publication as part of virus distribution presents severe threats to data processing in economy, public services and private life. IFIP General Assembly therefore passed a motion that every member society should appeal to its national legislative bodies to classify virus publication and distribution as a crime (the author will send the text of the IFIP resolution on request: VIRUSBAN.DOC: 56 lines, 3 kBytes).

Another controversy raised when Burger told the audience: 'My antivirus finds every virus'; unfortunately, he didnot accept a bet from the audience to prove his promise. Burger also said, that he needs only one hour to detect and eliminate any anomaly; this differed significantly from the 250 hours which according to Brunnstein are needed to analyse and classify a complex virus and

to produce the proper antivirus.

Some participants from the audience differentiated between good use of viruses and bad use. It could be Good Use of viruses against unacceptable activities, such as nuclear weapons or state activities such as census. Following such ideas, Wau Holland said that the existence of viruses gives a chance to analyse whether they are 'socially acceptable'.

The 'electronic newspaper', which reports the major discussions of CCC'89, was significantly more professionally organised than last year; it was produced by the team of CHALISTI, CCC's newly (1989) founded electronic newspaper, as edition no.4. Due to the minor foreign participation, most documents are German, with only two documents are written in English (Capt.Crunch's report on the Harper Hacker Conference, and the IFIP General Assembly's resolution on legal activities against viruses). There may be an English translation of the CCC newspaper in some time (?early February); I will send a short notice to PGN when this is available. People interested in the German version (1794 Lines,97 kBytes) or the English documents (135Lines,8 kBytes) can request it from the author.

Conclusion: CCC and its constituency is on the \*way to professionalism\*. On this way, CCC may loose control and even contact to real hacker groups, which they previously hold in cases such as Btx and NASA hack; in the KGB case, CCC evidently had neither information nor control of the crackers. On the other hand, CCC's propagation of UNIX enlarges the threats inherent in UUCP and the UNIXes.

Klaus Brunnstein    University of Hamburg, FRG    January 3, 1990



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 9: Issue 59

Wednesday 10 January 1990

## Contents

- [Drawbridge opens without warning in rush-hour traffic](#)  
[Jon Jacky](#)
- [Massive Electrical Failure in a Bus](#)  
[Peter Jones](#)
- [What hung the computer?](#)  
[Julian](#)
- [Passwords and security](#)  
[Phil Ritzenthaler](#)  
[Henry Spencer](#)  
[Jerry Leichter](#)  
[ark](#)  
[Peter da Silva](#)
- [IEEE Symposium on Research in Security and Privacy, Oakland 1990](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✉ Drawbridge opens without warning in rush-hour traffic

*Jon Jacky <JON@GAFFER.RAD.WASHINGTON.EDU>  
Tue, 9 Jan 1990 22:53:19 PST*

This isn't a computer incident, but it contains several system safety lessons that may be of interest to readers of this digest. The accident has been discussed in the Seattle papers almost every day since December 22. The following excerpts are from one of the stories that describe the cause, in THE SEATTLE TIMES, Monday January 8, 1990, p. 1:

TWO SHORTED WIRES JOINED TO CAUSE FATAL ACCIDENT, INSPECTORS SAY by Dick Lilly

... Engineers found that a screw driven into one wire and a short in another wire caused last month's fatal opening of the (Evergreen Point Floating Bridge's) drawspan.

(The inspectors will report) to the State Department of Transportation (DOT) on Friday, said Richard Hearth, one of two engineers from the consulting firm

of Parsons, Brinkerhof, Quade and Douglas Inc. who inspected the faulty Highway 520 bridge Saturday and yesterday.

The two shorted wires, one on the east drawspan and one on the west span, combined to send current around safety systems and lift the west section of the drawspan during a routine test December 22.

Several cars crashed into the unexpectedly rising bridge deck. ... One (driver) was killed. Five people were injured in the morning rush hour accident. ...

"Each fault individually did not cause the problem," said Patrick Buller, an electrical engineer from the (Washington State) Patrol who took part in the investigation. "It took both problems simultaneously for the bridge to rise," he said.

Power from the burned cable on the east drawspan probably reached the west side either through the metal of the bridge deck or along the metal walls of the submerged cables which connect the two movable spans with the control tower, said Daryl Rush, bridge maintenance supervisor for the DOT.

Picking up that current, the short on the west side, where 3/8-inch sheet metal screw holding an electrical box cover had pierced a wire, sent power to motors that lifted the west span, Hearth said.

The routine tests during which the accident occurred had until Dec. 22 been run almost weekly without incident for 18 years.

Ironically, it was a tiny heater designed to keep moisture from damaging circuits in an electrical relay that burned plastic insulation from one of the wires, causing the short circuit on the east span. Such heaters protect many of the bridge's electrical devices.

During a bridge opening, the device housing the burned wire senses the rotation of a gear in order to tell operators how far the east draw span has retracted.

At Step 10 in the 18-step dry-run test that was going on the day of the fatal accident, the device received power. Though the bridge does not open during any part of the test procedure, the shorted wire allowed power to reach motors on the west span.

For the Evergreen Point Bridge to open, grated sections of the bridge deck rise, allowing sections of the roadway to slide back for the passage of ships.

...

[ Here are further excerpts from THE SEATTLE POST-INTELLIGENCER, January 8, 1990, p. 1, ELECTRICAL SHORTS LIFTED SPAN by Mike Merrit ]

One move transportation officials made to ensure such an accident doesn't happen again is to stop the "dry run" tests of the bridge's control systems. Future tests will be done only with the span closed to traffic. ...

Hearth declined to comment on whether the bridge should have been designed with automatic mechanisms to prevent activation of its lift-deck motors unless the span was closed to traffic. "In hindsight, the question is a good one," (John)

Stevenson (assistant district administrator for DOT) said. "But when the design was being completed, it's hard to know what factors were taken into account. ... The span was built across Lake Washington in 1962.

... The west span short circuit, caused when a tiny screw touched wires inside a metal box, had probably existed for some months or years. The second short circuit ... had probably occurred gradually over several months or a year ... (a) heater apparently melted insulation from one of a bundle of wires. Sometime between tests run Dec. 15 and Dec. 22, when the malfunction occurred, enough insulation melted away to let the bare wire touch the metal cover plate.

... "The wire (with the melted insulation) is in such a place that it's not real visible," said Ernest Frye, who oversees inspections as the bridge's lead maintenance technician. ... (the assembly containing the wire) is inspected annually ... the latest inspection was April 9, 1989. But the damaged wire is one of a bundle of wires under a metal cover plate that is not usually removed in routine inspections.

Charles Mayhan, state moveable bridge engineer, said he did not do a detailed examination of the ... mechanism while inspecting the bridge earlier this year. "If I took the time to do all that, I wouldn't be able to do more than one bridge a year," he said.

[ The consulting engineers will recommend installation of devices to warn operators of short circuits ] Devices to detect small short circuits weren't widely used when the bridge was designed in the 1950's ...

- Jonathan Jacky, University of Washington

---

## **⚡ Massive Electrical Failure in a Bus**

*Peter Jones <MAINT@UQAM.bitnet>*

*Sun, 7 Jan 90 03:01:03 EST*

On Friday Jan 5, 1989, as I was returning from a day's skiing, the electrical system of the bus I was riding in suddenly went dead. The driver was forced to pull over on the side of the expressway. Subsequent investigation showed that the cause of the problem was a loose connection of the power cable leading to the starter. This cable can carry several hundred amperes of starting current; power is actually delivered to the starter motor via a nearby relay controlled by the ignition key. According to the driver, the cable came off a loose connection at the starter and shorted the high side of the battery to the bottom of the oil pan, burning a hole and spattering oil on the engine. Luckily, no fire resulted.

The driver got out and walked back to an emergency phone placed at the side of the highway. He returned, saying that instead of being connected to the police, he had heard a recorded message saying the phone was "not in a designated area", and giving another number to dial. But the phone had no dial on it!

A passing motorist was able to help the driver by relaying a message to the police. As a result, the bus company was notified, and sent another bus to get

us home.

Some further observations:

- 1) The headlights and AM/FM radio still worked after we pulled over, but not the rear flashers or rear lights. The driver put a flare behind the bus.
- 2) Installation of a two-way radio was planned for the following Monday. But I wonder if it could operate independently of the electrical system of the bus, in an emergency.
- 3) The extreme cold weather had ended, so that no-one felt cold.

The part that is computer system related is the part about the roadside phones giving an "error message" that the user could not respond to. I am reminded of the customer-operated touch-screen POS terminal reported in RISKS that gave a software error message and asked the user (customer) to hit return on a keyboard that presumably had only been present during testing.

I see this situation as a case of losing track of the system's behaviour as seen by the user. If you can get connected to a recording, then why not the police station? In a potentially life-threatening situation, no other system response is acceptable, in my view. Remember the Woody Allen film where an attempt to call the 911 police number results in an "all lines busy" voice recording, followed by a disconnect? This case was no joke. Nor did it seem to have been a failure of an individual phone, which wouldn't be worth mentioning in RISKS.

There's also the issue of the primary failure (electrical failure) resulting in a failure of systems to prevent further damage (the flashers).

So, while this tale appears marginally related to computers, I feel the system ergonomics and reliability design issues are very pertinent, and easy to visualize in this case.

Peter Jones MAINT@UQAM (514)-987-3542  
"Life's too short to try and fill up every minute of it" :-)

---

## ✂ What hung the computer?

<julian@riacs.edu>  
Tue, 09 Jan 90 23:16:55 -0800

A couple of nights ago I was working away merrily on my Macintosh with two cats plopped all over the table as usual. For some reason, while I was working in a usually reliable program, the computer froze. Couldn't figure it out; all I was doing was typing. While I was still thinking, the Mac suddenly unfroze, and the icon for the CDROM drive popped up on the desktop. It takes more than minute for this particular CDROM to come online, during which time the Macintosh is busied out, thus the inexplicable delay.

Who had pushed in the CDROM? A cat. One of them woke briefly, stretched, changed position, and in doing so shoved the disk into the drive. Since I am quite used to cats stretching I didn't bother to watch him and had no idea he needed the disk online. I was already cursing the software for crashing the

machine until the icon showed up.

Part of the blame for this confusion can be laid squarely on Apple. Their own Human Interface Guidelines specify that the pointer should be replaced with a watch for a "lengthy operation" (Inside Macintosh p.1-37). They often follow their own guidelines, but not in this case.

[Another hidden side-effect of the Unix "cat" command? If blank text had been inserted, you might have thought the system had gone tabby. Part of the problem is the emphasis on just "human" interfaces. But perhaps your cat now has a Macintush. Therein lies a tail. PGN]

---

**✉ Re: The risks of not learning (Password security, [RISKS-9.57](#))**

*Phil Ritzenthaler <phil@heinlein.cgrg.ohio-state.edu>*

*5 Jan 90 18:33:10 GMT*

> One student's answer: "Passwords have the advantage that it's easier to let  
> my friend use my account. If the system uses biometric devices for user  
> authentication, I have to be there when he logs in, to get him on to the  
> system. But, if the system uses passwords, I can just tell him my password,  
> and don't have to be there - he can login at his leisure."

GOOD LORD IN HEAVEN!! And these are going to be our System Managers and administrators of the FUTURE??

Heaven help us!!

Phil Ritzenthaler The Advanced Computing Center for the Arts & Design (ACCAD)  
Systems Manager The Ohio State University

---

**✉ Re: The risks of not learning?**

*<henry@utzoo.UUCP>*

*Tue, 9 Jan 90 14:58:28 EST*

>One student's answer: "Passwords have the advantage that it's easier to let  
>my friend use my account..."  
>So much for that one-week unit on 'Individual Accountability'.

I hope you also spent some time talking about how formal mechanisms often imperfectly capture the real nature of human organizations, and about the negative effects on security when overly-rigid formal mechanisms lead to the evolution of informal "bypass" mechanisms? This is a perfect example. Anyone who has ever loaned someone else a key knows that there *\*are\** real requirements for such things, accountability problems notwithstanding, when the overhead of "doing it right" is high.

Henry Spencer at U of Toronto Zoology

**✂ Re: Password sharing ([RISKS-9.58](#))**

<Leichter-Jerry@CS.YALE.EDU>

Tue, 9 Jan 90 16:20 EST

In an editorial remark added to my recent RISKS contribution, our Moderator writes:

If you want individual accountability, you do not share passwords. The telephone system is intrinsically vulnerable to illicit use of credit cards. If you wish to trust a friend, that may have low risk -- unless MANY people are involved; then you might like to have records that show who is actually using your resources....

This continues to miss the point I was making.

Consider the following two situations:

1. The system manager on my machine assigns a shared account to me and five other people (who, let us say for the sake of argument, are my friends).
2. I let the same five friends know what my password is.

Are these equivalent? The answer is absolutely not: While the "observable facts" may look the same - the same people have the same information - the RESPONSIBILITIES are radically different. In case 1, if one of the six people with access to the account abuse it, I will be able to deny responsibility - as will the five others. This is "lack of individual responsibility".

However, in case 2, if one of the six of us abuses the account, it is clear who bears the responsibility: Me. My five friends are acting as my agents, and I can complain all I like that it was they who acted - in giving them my password, I implicitly accepted the consequences of their actions.

Now, the problem is that those of us with an interest in security can easily see ourselves in case 1 - and we've learned that case 1 represents bad, if all too common, system management policy. (How many times have heard of systems in which each account costs money, so any number of users are assigned to the same account to keep the accountants happy?) However, we have much more difficulty imagining ourselves in case 2, since WE certainly would never let others know our password.

However it is exactly case 2 which we are discussing here! As long as it is understood that the "owner of record" of an account remains responsible for it no matter who he allows to use it - just as the owner of a telephone must pay the charges his friends run up on it - I can see no issue of "individual accountability" here.

The law, and our common sense of ethics, has been dealing with lending in this way for a long, long time. Why should computer accounts be treated in any different way? Admittedly, it may be worthwhile to point out to people that lending their accounts has a greater potential for abuse than lending their shirts, or whatever - exactly because passwords as a means of identification are freely reproducible. People understand this; they are more willing to lend

a key than to "lend" the combination to a lock.

-- Jerry

---

### ✉ Password sharing

<ark@research.att.com>

Tue, 9 Jan 90 21:02:15 EST

It has always seemed to me that there is no point in trying to prevent people from 'lending' their passwords to others -- they'll do it anyway.

A better administrative strategy might be to make it plain to people that they will be held responsible for any act committed under their login, whether they actually did it or not.

---

### ✉ Re: Password sharing ([RISKS-9.58](#))

<Postmaster@texbell.UUCP>

Wed, 10 Jan 90 10:09 CST

- > [Yes, some people are concerned about computer security and others are not
- > -- at least not until they've been burned. But Reality and Sensibility
- > are in this case two radically different things. If you want individual
- > accountability, you do not share passwords. ...

This is all true, but the amount of security you need depends on many things. For example, an account you pay money for might be a different matter than an account on a local BBS, which again is different from an account on a friend's UNIX box. Work and school accounts are another matter.

I wouldn't casually hand out passwords here at work, but I might give someone my compuserve password... and I'd change it later. I'd be even more likely to give someone a password for a local BBS, and probably wouldn't bother to change it.

Another variant is who you give the password to. You might be willing to swap passwords to class accounts at school, or project accounts at work, but you probably wouldn't hand out your CI\$ password to your co-workers.

So, having the ability to lend access to a resource is valuable, and is not always something to be feared. Security and convenience being opposed goals, it's important to gauge the level of security to the value of the resource in question.

Peter da Silva +1 713 274 5180

---

### ✉ Security and Privacy, Oakland 1990

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

Tue, 9 Jan 1990 15:15:37 PST

1990 IEEE Symposium on Research in Security and Privacy  
ADVANCE PROGRAM  
4 January 1990

MONDAY, MAY 7, 1990

0845-0900 Welcome, Introduction, Deborah Downs, Deborah Cooper

0900-1030 Commercial A1, Steve Lipner, Chair

Status Update

A VMM Security Kernel for the VAX Architecture, Paul Karger, Mary Ellen Zurko,  
Douglas W. Bonin, Andrew H. Mason

An Architecture for Practical Delegation in a Distributed System, Morrie  
Gasser, Ellen McDermott

Practical Authentication for Distributed Computing, John Linn

1100-1200 A1 SOS, Elizabeth Sullivan, Chair

The Army Secure Operating System, Neil Waldhart

Specification and Verification of the ASOS Kernel, Ben L. Di Vito, Paul H.  
Palmquist, Eric R. Anderson, Michael L. Johnston

1330-1500 Database I, Teresa Lunt, Chair

Integrating an Object-Oriented Data Model with Multilevel Security, Sushil  
Jajodia, Boris Kogan

A Little Knowledge Goes a Long Way: Fast Detection of Compromised Data in 2 D  
Tables, Dan Gusfield

Extending the Brewer-Nash Model to a Multilevel Context, Catherine Meadows

Rejoinder

Database II, Earl Boebert, Chair

Polyinstantiation and Integrity in Multilevel Relations, Sushil Jajodia, Ravi  
Sandhu

Naming and Grouping Privileges to Simplify Security Management in Large  
Databases, Robert W. Baldwin

Referential Secrecy, Rae K. Burns

Discussion

1730-1930 Reception

2000-2400 Poster Sessions, Hospitality Suite

TUESDAY, MAY 8, 1990

0900-1030 Information Flow, John Rushby

Information Flow in Nondeterministic Systems, J. Todd Wittbold, Dale M. Johnson

Constructively Using Noninterference to Analyze Systems, Todd Fine

Probabilistic Interference, James W. Gray, III

Security Models and Information Flow, John McLean

Rejoinder

1100-1200 Access Control and Integrity

Beyond the Pale of MAC and DAC -- Defining New Forms of Access Control,  
Catherine Jensen McCollum, Judith R. Messing, LouAnna Notargiacomo

Some Conundrums Concerning Separation of Duty, Michael J. Nash, Keith R.  
Poland

1330-1500 Authentication, Tom Berson, Chair

SP3 Peer Entity Identification, Bill Birnbaum

The Role of Trust in Protected Mail, Martha Branstad, W. Curtis Barker,  
Pamela Cochrane

A Security Architecture and Mechanism for Data Confidentiality in TCP/IP  
Protocols, Raju Ramaswamy

Reasoning about Belief in Cryptographic Protocols, Li Gong, Roger Needham,  
Raphael Yahalom

1530-1650 Verification, Deborah Cooper, Chair

The Deductive Theory Manager: A Knowledge Based System for Formal Verification,  
Ben Di Vito, Cristi Garvey, Davis Kwong, Alex Murray, Jane Solomon, Amy Wu

Formal Construction of Provably Secure Systems with Cartesiana, Heinz Brix,  
Albert Dietl

Verifying A Hardware Security Architecture, Joshua D. Guttman, Hai-Ping Ko

A Hierarchical Methodology for Verifying Microprogrammed Microprocessors

1700-1800 Technical Committee Business Meeting

2000-2400 Poster Sessions, Hospitality Suite

WEDNESDAY, MAY 9, 1990

0910-1020 Auditing and Intrusion Detection, Jim Anderson, Chair

The Auditing Facility for a VMM Security Kernel, Kenneth F. Seiden, Jeffrey P. Melanson

Adaptive Real-time Anomaly Detection Using Inductively Generated Sequential Patterns, Henry SI Teng, Kaihu Chen, Stephen C-Y Lu

Auditing the Use of Covert Storage Channels in Secure Systems, Shiu-Pyng Shieh, Virgil D. Gligor

1020-1030 Presentation of Awards

1030-1100 Break

1100-1200 Database III, Cristi Garvey, Chair

Transaction Processing in Multilevel-Secure Databases Using Replicated Architecture, Sushil Jajodia, Boris Kogan

Multiversion Concurrency Control for Multilevel Secure Database Systems, T.F. Keefe, W.T. Tsai

Modeling Security-Relevant Data Semantics, Gary W. Smith

1330-1700 Panel Discussions -- To Be Announced



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 9: Issue 60

Monday 15 January 1990

## Contents

- [The C3 legacy: top-down goes belly-up recursively](#)  
[Les Earnest](#)
- [Dispatchinate Computerized Cab Service](#)  
[PGN](#)
- [Risks of manual page formatters and inserted text](#)  
[J. Eric Townsend](#)
- [Re: What hung the computer?](#)  
[Dave Platt](#)
- [Perils of not planning for errors](#)  
[Ted Shapin](#)
- [Wrong 800 numbers](#)  
[Steven W. Grabhorn](#)
- [Password Sharing](#)  
[Dave Bafumo](#)
- [Call for papers for computer security foundations workshop](#)  
[John McLean](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✉ **The C3 legacy: top-down goes belly-up recursively**

*Les Earnest* <[LES@SAIL.Stanford.EDU](mailto:LES@SAIL.Stanford.EDU)>

10 Jan 90 1200 PST

After more than 30 years of accumulated evidence to the contrary, the U.S. Defense Department apparently still believes that so-called command-control-communications (C3) systems should be designed and built from the top down as fully integrated systems. While that approach may have some validity in the design of weapon systems, it simply doesn't work for systems intended to gather information, aid analysis, and disseminate decisions. The top-down approach has wasted billions of dollars so far, with more to come, apparently.

I noticed the citation in [RISKS 9.52](#) of the article, "The Pentagon's Botched Mission," in DATAMATION, Sept. 1 1989, which describes the latest development failures in the World Wide Military Command and Control System (WWMCCS). The

cited article indicates that they are still following the same misguided "total system" approach that helped me to decide to leave that project in 1965. I confess that it took me awhile to figure out just how misguided that approach is -- I helped design military computer systems for 11 years before deciding to do something else with my life.

In [RISKS 9.56](#), Dave Davis and Tom Reid observe that current C3 development projects seem to be sinking deeper into the mire of nonperformance even as the plans for these systems become more grandiose and unrealistic.

Please understand that I am not arguing against top-down analysis of organizational goals and functions. It is clearly essential to know which are the important responsibilities of an organization in order to properly prioritize efforts. Based on my experience, attempts at aiding analysis and decision-making tasks with computer applications should begin with the lowest levels and proceed upward IN THE CASES THAT WORK. Contrary to some widely held beliefs, many such tasks do not lend themselves to computer assistance and the sooner one weeds out the mistakes and intractable tasks the faster one can improve the areas that do lend themselves to automation and integration.

A great deal of time, effort, and money can be save by approaching development in an evolutionary bottom-up way. It is essential to shake-down, test, and improve lower level functions before trying to integrate at a higher level. Trying to do it all at once leads to gross instability that takes so long to resolve that the requirements change long before the initial version of the system is "finished." Each time one moves up a level it is usually necessary to redesign and modify some or all of the system. It is much faster to do that a number of times than it is to try to build a "total system" the first time because that approach almost never works.

Someone (Karl von Clausewitz?) once said that people who don't know history are condemned to repeat it. A modern corollary is that people who do know history will choose to repeat it as long as it is profitable. Unfortunately, the Defense Department's procurement policies often reward technical incompetence and charlatanism. I will support this claim with a few "peace stories" that would have been much more atrocious "war stories" if any of the systems that we designed had been involved in a real war. Fortunately, that didn't happen.

The presumption that computer-communication system development should be done on a grand scale from the outset is just one of many bad ideas that have taken root within the military-industrial establishment. The reason that this misconception has persisted for decades is that there is no penalty associated with failure. On the contrary, failures are often very profitable to the contractors -- the bigger, the better. The bureaucrats who initiate these fiascos usually move on before the project fails, so if anyone tries to point fingers they can say that it was the fault of the subsequent management.

While the "total system" approach is one of the more persistent causes of failure in C3 development, it is by no means the only misconception afloat. In subsequent segments I will review some other causes of historical fiascos. All of this will be ancient history, since I got out of this field about 25 years ago. Of course, many of the more recent fiascos are protected from public scrutiny anyway by the cloak of national security.

(Next segment: a SAGE beginning.)

-Les Earnest (Les@Sail.Stanford.edu)

---

## **✂ Dispatchinate Computerized Cab Service**

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

Mon, 15 Jan 1990 12:33:13 PST

Yellow Cab in San Francisco is using a dash-mounted computer in each taxicab to facilitate dispatching and supposedly to prevent dispatchers from favoring particular drivers. However, the system (\$800,000) ``remains plagued by breakdowns and by drivers grumbling that foul-ups mean a loss in income."

"When the system is on line, it works well," said Leon Collett, first vice president of the cab firm. "But we have had transmitter problems, hardware problems, software problems." ... [Computer Snarling Yellow Cabs in S.F., Maitland Zane, San Francisco Chronicle, 15 Jan 90, p.A2.]



J. Eric Townsend <jet@karazm.math.uh.edu>

Sun, 14 Jan 90 22:27:49 CDT

There's no horror story to go with this, we wised up in time...

Recently, we aquired two Sun SparcStation-1s. We only bought 1 100Mb drive for each from Sun and we're (still) waiting on shipment of our CDC drive. To save space, I only installed the basics: /, /usr, development tools, and a couple of other goodies. I did *\*not\** install the man pages, as they took up around 6Mb of badly needed space.

Then I had an idea: Mount /usr/man from our DECstation 3100 as /usr/man on the sparc-1s. It worked, and I sent mail to all accounts saying that the man pages were from Ultrix/BSD, and probably shouldn't be trusted in critical apps; they were just there for ease of remembering things like which ls(1) flag does what.

The next day there's mail telling me I've screwed up. There *\*are\** man pages for the sun, and I've mounted DEC3100:/usr/man pages over them. I typed "man ar", and sure enough, there were man pages with

Sun Release 4.0      Last change: RISC                      <pagenum>

at the bottom of each page... I was astounded. Luckily, the ar commands my prof needed must have been the same, as no data was lost, and everything worked. I dismounted all nfs, and looked at /usr/man -- nothing was there. "man ar" returned an error about not finding the man pages.

A little experimentation shows that the SunOS 4.0.3-4c man command

inserts the above line in the formatted man pages.

I think it's presuming a little too much to go ahead and cite the source/version of a manual page from within the formatting program...

J. Eric Townsend, University of Houston Dept. of Mathematics

---

**✉ Re: What hung the computer?**

*<dplatt@coherent.com>*

*Wed, 10 Jan 90 16:10:54 PST*

... It takes more than minute for this particular CDROM to come online, during which time the Macintosh is busied out, thus the inexplicable delay....

Part of the blame for this confusion can be laid squarely on Apple. Their own Human Interface Guidelines specify that the pointer should be replaced with a watch for a "lengthy operation" (Inside Macintosh p.1-37). They often follow their own guidelines, but not in this case.

This is probably one of those cases in which an implementation in one part of a complex system (the CD-ROM drivers) invalidated a simplifying assumption which had been made in another part of the system (the Finder).

During normal operations, it takes very little time for the Mac operating system to process a "disk mount" event. The current application (the Finder, in this case) calls MountVol(), which reads in the volume information and adds the necessary entry to the drive queue. The delay is usually less than a second, and so the Finder's author didn't consider it a "lengthy" operation which required putting up the stopwatch-cursor. There are a couple of circumstances in which this assumption turns out to be invalid, though. One of them is when the volume being mounted is a CD-ROM which adheres to the ISO 9660 standard.

The Mac operating system keeps track of the number of files available on each volume, and the Finder can display the counter. However, ISO 9660 CD-ROMs don't store this value in their headers. So, when you mount a new CD-ROM, the Mac's "Foreign File" code quite politely calculates the file-count, by stepping through the disk's directory! As you've noticed, this can take a loooooong time!

Unfortunately, there's no practical way for the Finder to tell that it's about to mount an ISO 9660 CD-ROM until *\_after\_* it has done so. >From the Finder's point of view, the MountVol() call is an atomic operation... one which takes a long time to return, it's true, but one which is not divisible into a look-first/do-it-now couplet. Hence, the Finder can't tell that it should [have] put up a stopwatch, until it's too late!

Fortunately, this issue will probably be moot when the new version of

the ISO 9660 Foreign File code is released by Apple. I've heard that Apple has eliminated the scan-the-directory-and-count-the-files process; it's too much work to do, for a small bit of information which is rarely used or useful.

Presumably, the new driver-code will be available through Apple dealers at no cost. It would be adding insult to injury for Apple to tell users that they'd have charge this Fur'in File code on their Apple Fee Line.

Dave Platt, Coherent Thought Inc. 3350 West Bayshore #205 Palo Alto CA 94303 8805

(415) 493-

---

### **⚡ Perils of not planning for errors**

*Ted Shapin <tshapin@orion.oac.uci.edu>*

*Fri, 12 Jan 90 10:36:55 -0800*

A large computer manufacturer (which my friend prefers remain anonymous) laid off 7% of its employees just before Labor Day.

My friend, who works there, and who I will refer to as 'Pat', was told he/she was not in the group to be terminated. However, when Pat called Saturday to get phone mail, Pat found his/her phone mail box no longer existed. Pat also could not log on to the company computer system. Needless to say, Pat was worried over the weekend. When Pat went to the plant on Tuesday, the magnetic badge would not open the computer-controlled door.

After some investigation, it turned out that a data entry operator had made some errors in entering employee numbers, and indeed Pat along with a few others in the same boat were still supposed to be employed.

It took 36 hours before all of Pat's computer-controlled privileges could be restored, (apparently, there was no procedure for correcting errors of this sort). Finally, some weeks later, Pat found that all of Pat's accrued vacation days had been reset to zero!

---

### **⚡ wrong 800 numbers**

*Steven W. Grabhorn <grabhorn@marlin.nosc.mil>*

*13 Jan 90 07:09:29 GMT*

Here's a short article on the risks of having an 800 number.

The 1/12/90 San Diego edition of the Los Angeles Times had the following article (first, a little background, Joan Kroc is having trouble finding a buyer for the San Diego Padres):

It started with a joking headline on Times sports editor Dave Distel's column on Thursday: "Have a Credit Card Ready and Call Now! 1-800-BUY-PADRES." Richard Cole, co-owner of Emslee Products of Cleveland, Ohio, is not laughing. His company sells sanitary napkins. Its number is 1-800-BUY-PADS. "Our phone

has been ringing all day," Cole said. "My secretary can't get any work done, I'm losing orders, I'm paying 12 cents per minute for every call, what in hell are you people doing out there?" [...]

Steve Grabhorn, Code 645, Naval Ocean Systems Center, San Diego, CA, 92152

---

### **✂ Password Sharing**

<DXB4769@RITVAX.BITNET>

Wed, 10 Jan 90 21:36 EST

It's the careless attitude that a computer password is no different than a house key that literally opens businesses and government to fraud and espionage.

The difference between loaning someone your house key and your password is simple. You own your house (or the bank does :) ), but your password and the resources that it protects are not yours, or yours to lend.

In addition, one loaned password can affect many people, even an organization, if abused - or misused, for that matter.

Lending and trust are key concepts in a democratic society, and important in social interaction. Yet in the electronic society that we live in, where a single password can affect people's lives, prudence and adherence to good security policies are just as important.

Dave Bafumo

Rochester Institute of Technology Criminal Justice/Computer Science (Student)

---

### **✂ call for papers for computer security foundations workshop**

<mclean@itd.nrl.navy.mil>

Wed, 10 Jan 90 17:28:31 EST

CALL FOR PAPERS

COMPUTER SECURITY FOUNDATIONS WORKSHOP III

June 12-14, 1990

Franconia, New Hampshire

The purpose of this workshop is to bring together researchers and practitioners in computer security to examine current theories of security in computing systems, with attention to the system models that provide context for such theories and techniques for verifying security as defined by these theories.

The workshop will include paper presentations, panel sessions, and participation in working groups. Papers and proposals for both panel sessions and working group problems are solicited in any application of formal methods from computer science, mathematics, and logic to computer security. Possible topics include security models, covert channel definition and analysis, information flow, access control, secure protocols, and verification techniques.

Instructions for Participants: Workshop attendance will be limited to thirty-five participants. Prospective participants should send four copies of a paper, panel proposal, or working group proposal to John McLean, Program Chair, at the address below. Submissions must be received by February 15, 1990. Participants will be notified of acceptance by March 15, 1990. Papers will be published in a proceedings that will be available at the workshop.

Program Committee:

Janice Glasgow Daryl McCullough Jon Millen  
Bob Morris Ravi Sandhu Marv Schaefer

For further information contact:

General Chair:	Program Chair:
Tom Haigh	John McLean
Secure Computing Technology Corp. Code 5540	
2855 Anthony Lane, Suite 130	Naval Research Laboratory
St. Anthony, MN 55418	Washington, DC 20375
(612) 782-7145	(202) 767-3852
haigh@dockmaster.arpa	mclean@itd.nrl.navy.mil

Publications Chair:

Bill Young  
Computational Logic, Inc.  
1717 W. 6thSt, Suite 290  
Austin, TX 78703  
(512) 322-9951  
young@cli.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 9: Issue 61

Saturday 20 January 1990

## Contents

- [Shortage of RISKS but no shortage of risks -- the week in review](#)  
[PGN](#)
- [AT&T Failure](#)  
[Bill Murray](#)  
[Jim Horning](#)
- [Risks of Voicemail systems that expect a human at the other end](#)  
[R. Aminzade](#)
- [Risks of vote counting](#)  
[Alayne McGregor](#)
- [Risks of supermarket checkout scanners](#)  
[David Marks](#)
- [European R&D in Road Transportation](#)  
[Brian Randell](#)
- [Old habits die hard](#)  
[Dave Horsfall](#)
- [Info on RISKS \(comp.risks\)](#)

---

## # Shortage of RISKS but no shortage of risks

*"Peter G. Neumann" <neumann@csl.sri.com>*  
*Fri, 19 Jan 1990 15:14:08 PST*

Well, it was a very strange week for me to be off-line, not to be able to report timely commentaries on the AT&T long-distance breakdown, several glitches aboard the shuttle Columbia, the Internet Worm trial of Robert T. Morris, and the San Jose CA indictment of three young computer people. On the other hand, most everything was well covered in the media, which had a field-week (= 5 field-days?).

The exact cause of the 15 Jan 90 AT&T slowdown is apparently still not known, although the result involved the propagation of bogus status information describing the partial outage of one network node, due to a software flaw. Apparently this information propagated to other nodes, and was amplified in

turn by each of them (because of the same program flaw?), creating the 'illusion' of a major outage. It should be noted that AT&T's service record up until that time had been exceptionally good, reflecting a fundamental concern for very high system availability. This outage immediately brought to mind (1) the article by Eric Rosen (Vulnerabilities of Network Control Protocols, ACM Software Engineering Notes, vol 6, no 1, January 1981) on the October 1980 four-hour collapse of the Arpanet, as a result of accidentally propagated bogus status messages that could not be garbage collected, and (2) the possibility of intentional insertion of a malicious effect. The latter possibility has been discounted by AT&T, but I observe somewhat tangentially that if an effect (e.g., a fault mode or vulnerability) can be triggered accidentally, in many cases it could alternatively have been caused intentionally. This was indeed the case in the Arpanet collapse, which was completely accidental.

The shuttle glitches included the spurious sounding of various alarms as well as the sudden rolling over of the spacecraft, among others.

The Morris trial awaits the final summations, the jury's decision, and the verdict, probably Monday or Tuesday.

The San Jose indictment involves three people accused varying of certain malicious computer-related and/or telephone-related security violations. This case will presumably drag on for a long time.

In each of these cases, RISKS will look forward to some definitive, nonspeculative reports, i.e., first-hand analyses by people involved, rather than just press clippings. The article by Eric Rosen on the Arpanet outage, noted above, and the article by Jack R. Garman, on the first shuttle synchronization problem, The Bug Heard 'Round the World, Software Engineering Notes, vol 6 no 5, October 1981, are superb examples of what I have in mind. Those of you who haven't seen those articles really should. They are absolutely required reading for all RISKS folks.

Our sendmail time-out multiple-copy problem may or may not still exist (I believe all known fixes and some other hopeful improvements have been installed). However, several of you suffered multiple copies of [RISKS-9.59](#), apparently because of a gateway glitch caused by someone's overflowing mailbox. (I continue to further subpartitioned the mailing list, in an attempt to isolate or minimize the problem, but even with small sublists it seems to continue sporadically.) I apologize for the frustration that results from multiple copies. My own frustration is most considerable when I cannot do anything about the problem.

Above all, the difficulties of getting concurrent processing programs flaw-free is illustrated by almost all of the above-mentioned cases, the AT&T slowdown, the Internet Worm, the first shuttle synchronization problem, and the Arpanet collapse. PGN

---

## **AT&T Failure**

<WHMurray.Catwalk@DOCKMASTER.NCSC.MIL [WHMurray@DOCKMASTER.ARPA]>  
Wed, 17 Jan 90 09:37 EST

The assertion by AT&T, "in an effort to allay customer fears about the networks reliability," that the outage was "traced to a single computer program," not only fails to reassure me, but alarms me greatly. It suggests a serious failure on their part to understand the nature of the problem.

While the proximate cause of this problem was an error in the design or implementation of a single program, the actual cause is a system that is unable to isolate failing components, and indeed that specifically designed to propagate the failures in such a way as to cause the failure of the entire system.

This is the second event in as many years to demonstrate the failure of the new telephone system to cope with the challenges that confront it. If, on the day before the Hinsdale fire, you had asked me if the failure of a single central office could cause the loss of all long distance service to 350,000 subscribers, I would have said "No, we do not build telephone systems that way. You might lose access to one carrier, but you would retain access to the others." Never would I have imagined that Illinois Bell, only partially in response to the equal access requirements, would centralize all access to all carriers in a single unattended central office.

Likewise, if on Sunday, you had asked me if a change, error, or manipulation of a single program in a single switch could bring down the entire AT&T network, I would have been happy to reassure you that such could not happen. AT&T has been the leader in teaching the rest of the world how to avoid such failures. While an authorized programmer, or even a hacker, might be able to affect a single switch, the system is specifically designed to prevent the effect from propagating. Little did know; little would I have believed.

If AT&T management actually believes its press releases, if they are not simply propaganda designed to comfort the sheep, then it truly bodes ill for our world economy. Of course, part of the difficulty with such propaganda is that you might yourself forget that that was what it was. In a large organization like AT&T, it is likely that at least some of your employees will be taken in.

I recognize that there are limits to our ability to identify and isolate failing components, that at some point further attempts to do so become self-defeating. If AT&T were claiming that this event was, similar to the second great Northeastern blackout, caused by, or even in spite of, such measures, I would be less alarmed. What concerns me is the pretense that such a failure is so anomalous that special precautions or design considerations are not indicated.

William Hugh Murray, Ernst & Young

---

### **Telephone malpractice?**

*Jim Horning*

*16 Jan 1990 1108-PST (Tuesday)*

Did you have trouble completing long-distance calls yesterday? Maybe you should sue AT&T for malpractice. Consider the following Congressional testimony (on the topic of SDI software) from Solomon J. Buchsbaum, Executive Vice President, Customer Systems, AT&T Bell Laboratories, December 3, 1985:

Some critics have specifically questioned if it is possible to generate great quantities of {\it error-free} software for the system, and to ensure that it is, indeed, {\it error-free software.}

This is the wrong question. ... Software is always part of a larger system that includes hardware, communications, data, procedures, and people.

The right question, as well as the key issue, is the broader one of whether the total BM/C3 system can be designed to be robust and resilient in a changing and error-prone environment. The key, then, is not whether the software contains errors, but how the whole system compensates for such errors as well as for possible subsystem failures. ...

Can such a large, robust, and resilient system be designed--and not only designed, but built, tested, deployed, operated and further evolved and improved? I believe the answer is yes. I seem confident of this answer because most if not all of the essential attributes of the BM/C3 system have, I believe, been demonstrated in comparable terrestrial systems.

The system most applicable to the issues at hand is the U.S. Public Telecommunications Network. ...

There are three keys to achieving high reliability, availability, maintainability, and adaptability.

The first is the use of distributed architectures both for the entire network and for major systems within the network. The approach compartmentalizes crucial functions in modules throughout the country ...

The second key is the use of redundancy, again both in the entire network and in the component systems. And the third key is the coupling together, the integration, of all the component systems by means of well-specified, well-controlled interfaces.

The network as a whole is much more reliable than its individual components. That's because the network is designed to be fault tolerant. It continuously and automatically checks its own condition. When a problem is detected, it isolates the faulty component, so that the network can continue to function using a substitute or redundant component.

For high availability, the public telecommunications network is designed to work at its specified level of performance even when some of its component elements are unavailable. ...

... This approach not only reduces software complexity. It also permits the fullest use of software as a strength, enhancing network flexibility and resiliency.

Perhaps Dr. Buchsbaum envisioned an SDI that might for a significant fraction

of a day tell over half the incoming ICBMs "We can't handle you right now, please keep trying"?

Perhaps Dr. Teller thinks that the problem would go away if we just gave everyone a Brilliant Telephone?

Jim H.

---

## **✶ Risks of Voicemail systems that expect a human at the other end**

*<r.aminzade@lynx.northeastern.edu>*

*Thu, 18 Jan 90 08:24:18 EST*

Last night my car had a dead battery (I left the lights on -- something that a very simple piece of digital circuitry could have prevented, but I digress), so I called AAA road service. I noted that they had installed a new digital routing system for phone calls. "If you are cancelling a service call press 1, if this is an inquiry about an existing service call, Press 2, if this is a new service call, Press 3." All well and good, except that when I finally reached a real operator, she informed me that the towtruck would arrive "within 90 minutes." In less than the proposed hour and a half I managed to beg jumper cables off of an innocent passerby and get the car started, so I decided to call AAA and cancel the service call.

I dialed, pressed 1 as instructed, and waited. The reader should realize that my car was illegally parked (this is Boston), running (I wasn't going to get stuck with a dead battery again!), and had the keys in the ignition. I was not patient. I waited about four minutes, then tried again. Same result. I was now out of dimes, but I noticed that the AAA machine began its message with "we will accept your collect call..." so I decided to call collect.

Surprise! I discovered that New England Telephone had just installed its digital system for collect calls. It is quite sophisticated, using some kind of voice recognition circuit. The caller dials the usual 0-(phone number), and then is asked "If you wish to make a collect call, press 1...If you wish to..." Then the recording asks "please say your name." The intended recipient of the collect call then gets a call that begins "Will you accept a collect call from <recording of caller stating his name>"

I knew what was coming, but I didn't want to miss this experience. I gave my name as something like "Russell, Goddammit!," and NET's machine began asking AAA's machine if it would accept a collect call (which it had already, plain to the human ear, said it would accept) from "Russell Goddammit!". Ms. NET (why are these always female voices?) kept telling Ms. AAA "I'm sorry, I don't understand you, please answer yes or no," but Ms. AAA went blithely on with her spiel, instructing Ms. NET which buttons to push.

I stood at the phone (car still running...machines nattering away at each other) wondering who could do this episode justice. Kafka? Orwell? Groucho? I was sure that one machine or the other would eventually give up and turned things over to a human being, but, I finally decided to dial a human operator,

and subject the poor woman to a stream of abuse. She connected me to AAA, where I punched 3 (rather than the appropriate but obviously malfunctioning 1), and subjected yet another underpaid clerk to my wrath.

---

## risks of vote counting

*Alayne McGregor*

*Fri, 19 Jan 90 14:40:17 EST*

High-tech vote counting unreliable, city decides  
<Toronto Globe and Mail (Dec. 16, 1989)>

In the wake of a chaotic election last year, the first Canadian city to use sophisticated electronic-voting machines is going back to counting votes the old-fashioned way. By a 13-3 vote, Toronto politicians decided yesterday to sell more than \$1.6-million worth of optical scanning machines bought for the November, 1988, municipal election. That race was marred by a recount brought about by the discovery that 1,408 ballots had been improperly handled by the machines.

More than a year later, the election is still not over. On Monday, a court-ordered recount is to be held in the Wards 3 and 4 separate school trustee race. [In Ontario, separate == Roman Catholic.] The council's decision flew in the face of a task force proposal, put forward before Council yesterday, to double the number of electronic voting machines, to 500 from 250, in time for the next election. It would have cost an additional \$1.6-million.

Not only are the machines more efficient, they are more accurate and provide quicker results at the end of the day, said Martin Silva, who headed an elections task force set up last year. "There's nothing wrong with the machines," Mr. Silva said in an interview. He attributed the election problems to the previous council's decision to buy only half the number of machines needed.

Toronto was the first Canadian city to use the optical scanning machines, in a by-election before the 1988 election, said an official in the city clerk's department. It is also the first to get rid of them, he said.

Other cities using the same machines include North York and Vancouver. A similar system is also used in Scarborough and Etobicoke, said Robert Clark, director of legislative services in the Toronto clerk's department.

=====

A few comments:

>From my experiences in working for candidates in many elections (municipal, provincial, and federal), I would say that it's not just optical scanning machines that get confused by ballots. Manual counting depends on the quality of the people doing the counting. Given that poll clerks and Deputy Returning Officers (the people who actually count the votes on election day) are patronage appointments (in Canada), I'm not too hopeful.

And there are the confused rules: Here in Ottawa, we had endless recounts in one city ward election (first one candidate was declared the winner, then the other). It finally had to be settled by a new election (won convincingly by one candidate, thank heavens), after the last recount declared a tie. And what was one of the big issues in the recounts: whether a "happy face" beside a candidate was a vote for that candidate!

---

## **✂ Risks of supermarket checkout scanners**

*David Marks*

*19 Jan 90 16:33:23 GMT*

The following appeared in the BUSINESS BRIEFING section of the 22 January 1990 issue of INSIGHT magazine:

"Supermarket shoppers would be wise to keep a watchful eye as their purchases are passed over the checkout scanning systems used in most stores, says the New York State Department of Agriculture. The agency reported last month that inspections of 33 stores with electronic checkout showed that all but one overcharged their customers.

'It is in the shoppers' best interest to check that the prices they are being charged are those that are being advertised,' says department spokesman Gerald Moore. The problem, he adds, is that 'scanners are only as accurate as the people who program them.' The department contends that stores are not reprogramming the computerized price scanners frequently enough to reflect sales and other price changes. Inspectors posing as customers and purchasing some 150 items in each store were overcharged for 3 percent on average. The department kept no tally of whether inspectors were overcharged.

Retailers contend that just as many pricing errors are made in favor of the customer and that overall accuracy of scanning systems is superior to conventional cashier checkout. 'Consumers would not accept the technology if they felt it was inaccurate,' says Peter Larkin, spokesman for the Food Marketing Institute, a grocery trade group. To ease consumer anxiety about the technology, many supermarkets offer a guarantee that backs up the accuracy with product giveaways for items consumers find overpriced by the scanner.

Whether customers come out even in the end is not the issue according to Moore. 'It shouldn't be a crapshoot. People should be charged what is advertised.'"

I seems to me that consumers accept the technology not because they feel it is accurate, but because it makes checkout faster. Also, where I live Kroger gives your money back on items that are not charged the price marked on the shelf. However, this still puts the burden on the customer. In the

"old days," you could check the price marked on the product against the one rung up. Now you have to write down the price on the shelf and compare it at the checkout. When there are lots of people impatiently waiting in line behind you, are you really going to do that?

David J. Marks M/S 3520 Texas Instruments, Johnson City, TN. 37605

---

## ✶ European R&D in Road Transportation

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

*Thu, 18 Jan 90 17:58:04 BST*

Today's Guardian Newspaper contains an article by Rex Malik, a well-known UK commentator on the computer scene, entitled "Every Move You Make ...", discussing possible implications of two current European R&D initiatives concerning the use of computers in road transportation, DRIVE and PROMETHEUS. As I understand it, DRIVE is an EC (European Community) initiative that has been largely motivated by concerns about social and environmental impacts of road traffic, whereas PROMETHEUS is a EUREKA project (which means that it is collaboratively sponsored by various European national governments directly) that is backed mainly by the automotive manufacturers.

Brian Randell, Computing Laboratory, University of Newcastle upon Tyne, UK

PS: Some years ago Malik authored a book entitled "And Tomorrow .. The World? Inside IBM" (Millington, London, 1975), which - how shall I put it - redressed the somewhat uncritical view of IBM to be found in Thomas J. Watson Jr's "A Business And Its Beliefs: The Ideas That helped build IBM" (McGraw-Hill, New York 1963). I recommend both - but only if read together! (This "recommendation" is not intended to have any specific explicit relevance to RISKS :-)

=====

Contracts for the EC's Drive (Dedicated Road Infrastructure for Vehicle Safety in Europe) programme preliminary phase were awarded earlier this year....

...

Drive is a major EC pre-competitive research and development programme. It is almost a cousin of the EC's Esprit, and it is likely to have radical consequences.

...

Drive is an attempt to work out how to use information technology to create the infra-structure needed to help reduce the EC's road accident-related death and injury figures, (currently around 55,000 of the former and 350,000 of the latter), reduce environmental pollution and improve road traffic efficiency by enmeshing the road system in a web of IT.

That's the radical bit.

The parallel Prometheus programme aims to add electronics - automatic guidance and navigation systems - to vehicles, creating "smart cars" permanently linked to the Drive traffic environment management control systems.

The long-term aim is to transform driving and driving conditions. But when put in the context of other trends, these technical developments may have different connotations.

The initial Drive contracts are for the specification phase. Proposal T416, for example, is for a "Black Box", a Vehicle Journey Data Recorder - an improved digital version of the tachographs which monitor the driving times of professional drivers.

But T416 goes much further. It aims to produce a record for non-professional drivers giving the exact trajectory of a vehicle during the last 1,000 meters preceding an accident.

This system is likely to operate within a road management environment in which vehicles will be linked at all times via a radio telecommunications network which will provide information about routes and traffic conditions - which, in the longer term, may over-ride systems of driver control.

It could effectively turn vehicles into part of instantly assembled or disassembled what-you-might-call electronically-coupled trains.

It could also provide a running record that we lawfully behave by recording in real time where and who we are when we leave our own private world and enter society's.

This traffic management environment will operate across national frontiers. You thought you could get away? You thought wrong. Orwell may well have been right in intent even if he wasn't with the date, technology or politics.

We are, with the best of motives - what after all could be a better motive than the saving of lives in massive numbers? - and for the greatest good of the greatest number (where have I heard that before?) creating the conditions which underlie the Orwellian nightmare.

Whether we operate them in the Orwellian way is, of course, a different issue.

...

---

## **✘ Old habits die hard**

*Dave Horsfall <dave@stcns3.stc.oz.au>  
Thu, 18 Jan 90 09:15:42 est*

Taken from the "Sydney Morning Herald" 15 Jan 90:

``A [Sydney] reader recalls his time in Zimbabwe, when computer setting was installed at the country's main commercial printers. A supervisor from the hot-metal printing days had always used a mallet to jog the linotype machines back into action, and found that old habits die hard. The result? A technician flown in from Johannesburg to repair a badly bruised computer."`

[ Not so much a risk to the public from computers as a risk to the computer from the public, I guess ]

Dave Horsfall (VK2KFU), Alcatel STC Australia, [dave@stcns3.stc.oz.au](mailto:dave@stcns3.stc.oz.au)



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

**Volume 9: Issue 62**

**Friday 26 January 1990**

## Contents

- [Australian medical database linkages](#)  
[Michael Bednarek](#)
- [Cause of AT&T network failure](#)  
"Telephony"  
[Jim Harkins](#)
- [London Stock Market Disruption](#)  
courtesy of [Steve Milunovic](#)
- [Railway interlocking](#)  
[Clive Feather](#)
- [More risks to computers](#)  
[Richard Thomsen](#)
- [Re: Risks of supermarket checkout scanners](#)  
[Marvin Moskowitz](#)  
[Doug Renner](#)  
[Don Craig](#)
- [Robert T. Morris Convicted](#)  
[Michael J. Chinni](#)
- [Advance Program for Oakland Symposium \(REVISED\)](#)  
[Debbie Cooper](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ***⚡* Australian medical database linkages**

*Michael Bednarek, Melbourne University <U3369429@ucsvc.unimelb.edu.au>  
Tue, 23 Jan 90 13:32 +1100*

Database `akin to ID card'  
by Tony Healy  
(The Australian, 23-Jan-1990)

Incensed pharmacists have forced the deferral of a nationwide computer network which they say has many features of the Australia Card. [A national ID card scheme whose introduction was recently abandoned] According to confidential documents obtained by The Australian, the proposed network will record

every medical prescription issued to every individual and family in Australia during long periods of time. It will thus form a detailed and easily accessed record of personal illness and disease.

Although the network has received little publicity, it was originally scheduled to start operating on a pilot basis in April and to be fully operational by the end of the year. It is to be implemented by the same government body that wanted the Australia Card -- the Health Insurance Commission -- using the same computers it bought for the Australia Card.

Most controversial of all is the commission's intention to link its database with that of the Department of Social Security. This intention is explicitly stated in the documents held by \_The Australian\_ -- a Health Insurance Commission report titled Strategy Proposal for the Management of the Pharmaceutical Benefits Program.

In the report, the commission also proposes making its network available on a commercial basis to pharmaceutical suppliers. Such a link realises the worst fears of civil libertarians, who contend that the centralisation of information and high speed access exposes information to abuse.

Both the Pharmacy Guild and the Australian Medical Association (AMA) have objected to the risk this poses to patient confidentiality. Guild protests forced the commission to postpone the introduction of the network by six months., its president, Mr Jim Mathews, said.

The federal president of the AMA, Dr Bryce Philips, said the association has sought formal assurances from the commission that patient confidentiality can be guaranteed. "If it can't, we will not be part of it," he said. A pointer to the furtiveness surrounding the network is that the AMA learned about it only by chance late last year, Mr Mathews said. In its report, the Health Commission also states its intention to create a culture in which people carry an identifying card.

Confidential tender documents issued by the commission call for the network eventually to be able to accept magnetic stripe cards. In addition, the commission recently tried to expand the information it gathers from concession application forms.

Pharmacists point out that the extra information gives the Government the same information it wanted to record on the Australia Card and have refused to provide it.

The rationale behind the network is to reduce an estimated \$[AUS]30 million worth of pharmacy benefits fraud identified in report by the Attorney General.

The network will consist of online terminals in each of Australia's 5500 pharmacies, connected to a central database running on the commission's two IBM 3090 mainframes.

Before issuing prescriptions, pharmacists will be required to check all customers on the computer. A principal reason is their eligibility for pensioner and other concessions -- this concerns about 80 per cent of prescription customers.

A spokesman for the Federal Minister for Community Services, Mr Staples, denied the claims and described them as part of pharmacists' heated campaign against the Government.

Michael Bednarek, Big River Ski Lodge Caravan Park, Seelands via  
Grafton NSW 2460, Australia, Phone: +61 66 {44 9324 | 44 9200}  
u3369429@{murdu.oz.au | ucsvc.dn.mu.oz.au} | mb@munnari.oz.au

[Also submitted by ph@wolfen.cc.uow.oz.au (Rev Dr Phil Herring) ]

---

## **✂ Cause of AT&T network failure**

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

*Fri, 26 Jan 90 14:24:30 PST*

From Telephony, Jan 22, 1990 p11:

"The fault was in the code" of the new software that AT&T loaded into front-end processors of all 114 of its 4ESS switching systems in mid-December, said Larry Seese, AT&T's director of technology development. In detail:

The problem began the afternoon of Jan 15 when a piece of trunk interface equipment developed internal problems for reasons that have yet to be determined. The equipment told the 4ESS switch in New York that it was having problems and couldn't correct the fault. "The recovery code is written so that the processor will run corrective initialization on the equipment. That takes four to six seconds. At the same time, new calls are stopped from coming into the switch." Seese said.

The New York switch sent a message to all the other 4ESS switches it is linked with that it was not accepting additional traffic. Seese referred to that message as a "congestion signal." After the switch successfully completed the reinitialization, the New York switch went back in service and began processing calls. That is when the fault in the new software reared its ugly head. Under the previous system, switch A would send out a message that it was working again, and switch B would double-check that switch A was back in service. With the new software, switch A begins processing calls and sends out call routing signals. The reappearance of traffic from switch A is supposed to tell switch B that A is working again.

"We made an improvement in the way we react to those messages so we can react more quickly. The first common channel signaling system 7 initial address message (caused by a call attempt) that switch B receives from switch A alerts B that A is back in service. Switch B then resets its internal logic to indicate that A is back in service," said Seese.

The problem occurred when switch B got a second call-attempt message from A while it was in the process of resetting its internal logic.

"[The message] confused the software. it tried to execute an instruction that didn't make any sense. The software told switch B 'My CCS7 processor is insane'", so switch B shut itself down to avoid spreading the problem, Seese explained.

Unfortunately, switch B then sent a message to other switches that it was out of service and wasn't accepting additional traffic. Once switch B reset itself and began operating again, it sent out call processing messages via the CCS7 link. That caused identical failures around the nation as other 4ESS switches got second messages from switch B while they were in the process of resetting their internal logic to indicate switch B was working again.

"It was a chain reaction. Any switch that was connected to B was put into the same condition."

"The event just repeated itself in every [4ESS] switch over and over again. If the switches hadn't gotten a second message while resetting, there would have been no problem. If the messages had been received farther apart, it would not have triggered the problem."

AT&T solved the problem by reducing the messaging load of the CCS7 network. That allowed the switches to rest themselves and the network to stabilize.

---

### **✉ Re: AT&T Failure**

*Jim Harkins <jharkins@sagpd1.UUCP>  
23 Jan 90 12:39:43 PST (Tue)*

WHMurray.Catwalk@DOCKMASTER.NCSC.MIL [WHMurray@DOCKMASTER.ARPA] says  
>The assertion by AT&T, "in an effort to allay customer fears about the networks  
>reliability," that the outage was "traced to a single computer program," not  
>only fails to reassure me, but alarms me greatly. It suggests a serious  
>failure on their part to understand the nature of the problem.

I think you need to remember that this failure report was intended for the great unwashed, who relate the term 'computer' to their Apple II, or possibly the protagonist in the movie 'The Demon Seed'. It is clearly inadequate for those of us who are technically literate. I for one am looking forward to reading in Risks and similar technical journals what really happened.

jim

---

### **✉ London Stock Market Disruption**

*Steve Milunovic <Steve\_Milunovic@quikmail.sri.com>  
26 Jan 90 09:37:59*

Trading on the London Stock Exchange suffered a minor disruption on 23 Jan 90

when a computer problem interrupted the quotation of the stock exchange market indexes for two hours and 20 minutes. The problem was spotted when The Financial Times-Stock Exchange index of 100 leading stocks suddenly went from a slight gain to a noticeable loss. The exchange shut down the index service at noon, installed a standby computer and began operating the service again at 2:20 p.m. The exchange's automated computerized trading system was not affected, and individual stock quotes were accurate. [Source: N.Y. Times News Service, 23 Jan 90]

---

## ✂ Railway interlocking

Clive Feather <clive@ixi.UUCP>

Tue, 23 Jan 90 10:08:23 gmt

I felt I had to say a few things about Douglas Jones' item in [RISKS 9.58](#). Whilst I realise that UK and US usages may be different, I think that some of these points may be of interest to all readers anyway.

> (One at a time because it takes his full strength ...)

Some levers control the signal or points electrically, and so require almost no effort. For this reason, the lever handle is cut short so that only one hand can be used on the lever. Nevertheless, the signalman will only operate one lever at a time.

In large boxes, two or three signalmen may work a single frame ("frame" is the UK term for the row of levers). In this case, it is possible for two or more levers to be operated at the same time. This was a contributing factor to the accident at Hull (Paragon).

[Note to PGN: msb@sq.com mailed you and me a description of this about two years ago. If you or he still has it, it might be worth posting it to RISKS.]

> (I've seen photos ... with banks of 20 or more control levers.)

In the UK, 20 levers would be regarded as a small frame (and so low paid!). A typical main-line box would have 50 to 60 levers, and a large one could have two frames of 120 levers each. This makes the interlocking problem considerably more complex.

> ... thus, there are 256 possible states of the system.

> An interlocking machine consists of a set of 8 transverse rods crossing 8

> rods linked to the control levers.

It would be unusual for there to be exactly 8 transverse rods, or "tappets" as they are known. Each tappet implements one condition in the interlocking. It is not sufficient to consider the static states, as there are many circumstances when a \*change\* must be forbidden (e.g. don't move 2 if 1 is up, even though either state of 2 is legal when 1 is up). In the example given, the conditions, one per tappet, would be:

1, 3, 4 down to move 2

5, 6, 8 down to move 7

3 up only if 2 set to straight through

4 up only if 2 set to loop

- 5 up only if 7 set to straight through
- 6 up only if 7 set to loop
- 1 up only if 3 and 4 down
- 8 up only if 5 and 6 down
- 1 and 8 cannot both be up

Thus 9 tappets would be required. (The last condition implements a general rule that trains are never allowed into a passing loop from both directions at the same time).

(Of course, this layout would not be implemented as such. Firstly, the points would have locks, each controlled by their own lever. Secondly, two further signals would be placed at the same locations as 1 and 8, but applying in the opposite direction, so that a train can be shunted between the two sides of the loop without leaving the area controlled by the signal box. Thirdly, these two signals would be electrically interlocked with equipment which ensures that a train cannot be signalled on to a single line which is already occupied. Fourthly, there would be distant signals about a mile before 1 and 8, which show only "caution" and "clear"; these could only show clear if the points are set for straight through running, and all signals in that direction are at "go". Finally, a King lever would be installed to allow the box to be unmanned at night; when the lever is pulled, it is possible to clear the signals in both directions at the same time, notwithstanding the interlocking, and the signal boxes on either side would be connected to each other as if this one was not there. So in fact we would have 13 levers, probably about 18 tappets (I haven't worked it out), and some electrical interlocks (see below). But this is starting to sound like rec.railroad :-)

Modern practice in lever frames (which are slowly being phased out) is to use electrically controlled bolts as well as or instead of tappets to lock the levers. This allows practices such as:

- don't allow a signal to be raised without permission from the next signal box down the line;
- ensure that permission applies for "one pull only", and that the signal must be replaced before permission can be given again;
- only allow the exit signal to be raised if a "token" has been issued for the single line section ahead; two signal boxes are connected so that only one token can be issued at a time (the token may be physical or logical);
- ensure that a train has occupied and cleared a specific track circuit before the signal can be cleared again ("Welwyn control").

The Farnley Junction accident ([RISKS-5.66](#), 30 Nov 87) shows that safety critical software problems are nothing new (the accident occurred because NOT NOT X equals X), and railways do indeed have something to teach us.

Clive D.W. Feather, IXI Limited ...!uunet!uk!ixi!clive (riskier)

---

## More risks to computers

Richard Thomsen <rgt%beta@LANL.GOV>

Mon, 22 Jan 90 08:25:52 MST

A friend of mine worked as a computer operator in a company with a large IBM computer. One day, they called in the repairman for a faulty console. When the repairman arrived to check out the problem, he noticed that some of the keys of the console keyboard were stuck down, in the shape of a closed fist. His comment: "We can fix this, but it will not be under warranty."

Richard Thomsen

---

**✂ Re: Risks of supermarket checkout scanners (Marks, [RISKS-9.61](#))**

Marvin Moskowitz <marvinm@ttidca.TTI.COM>

22 Jan 90 23:47:21 GMT

>I seems to me that consumers accept the technology not because they feel  
>it is accurate, but because it makes checkout faster.

It seems to me that consumers accept the technology because they have no choice. The only markets in Los Angeles that DON'T use automated scanners are small convenience stores (e.g. 7-11). If you want to buy food, you HAVE to accept the scanner system. My wife has objected to the lack of marked prices, preventing her from checking the receipts. I have suggested she take a pen to the market and mark the prices as they come off the shelf. The only problem is a fair percentage of the shelf prices are missing, which I imagine IS a violation of some law. Go tilt at windmills!

Marvin S. Moskowitz, Citicorp/TTI, 3100 Ocean Park Blvd., Santa Monica, CA 90405  
(213) 450 9111 x3197 {philabs|csun|psivax}!ttidca!marvinm

---

**✂ Re: risks of supermarket checkout scanners**

Doug Renner <elec@pnet51.orb.mn.org>

Tue, 23 Jan 90 11:48:30 CST

It may very well be the case that people accept the technology because they feel it is more accurate. The real issue is that this 'feeling' may be unfounded, or based primarily on marketing hype.

UUCP: {amdahl!bungia, uunet!rosevax, chinnet, killer}!orbit!pnet51!elec  
ARPA: crash!orbit!pnet51!elec@nosc.mil INET: elec@pnet51.cts.com

---

**✂ Re: Risks of supermarket checkout scanners**

Don Craig <dmc@tv.tv.tek.com>

Mon, 22 Jan 90 16:11:44 PST

David Marks quotes an INSIGHT magazine article: "Retailers contend that just as many pricing errors are made in favor of the customer..." What then should the attentive shopper, checking his prices, do when he sees an UNDERcharge go past? My conscience is regularly stricken when I shop at the local purveyor of

organic and transitional organic foodstuffs. Service ranges from pleasant and ineffectual through bossy and dumb, checkout pricing is by seminumerate human being. I buy Thomas Hardy's ale there, which costs \$2.89 for a 6 ounce bottle, or \$11.56 for a carton of 4. Each bottle is marked \$2.89, but the carton price appears nowhere. If asked by the checkout clerk I tell them the price is \$11.56, but if they don't ask I accept what they charge. About half the time, it's \$2.89 for the whole carton. I tell myself this makes up for the utter incompetence of say, the organic meat department, but I still feel guilty when I leave. What should I do? ...Distressed in Oregon

[Perhaps it is really Oregonic meat, not Organic meat, and someone is illiterate as well as innumerate. Perhaps you should switch to Samuel Adams beer. Although Hardy was more literate, Adams might have been more patriotic. But you could have a nice chat with the manager. You will probably find that the hearty ale is not Bar Coded. (HardyHar at your neighborhood bar.) PGN]

---

### **✂ Robert T. Morris Convicted**

*"Michael J. Chinni, SMCAR-CCS-E" <mchinni@PICA.ARMY.MIL>  
Tue, 23 Jan 90 9:52:55 EST*

The following is an excerpt from a message sent by one of our computer security people. Michael J. Chinni, Picatinny Arsenal, New Jersey

Verdict: "GUILTY"

Student "worm" whiz is found guilty. A U.S. court jury returned its verdict about 9:30 pm after approximately six hours of deliberation. Robert T. Morris was found guilty of federal computer tampering charges for unleashing a rogue program that crippled a nationwide computer network (Internet system). A date for sentencing has not yet been set. Morris faces up to five years in prison and a \$250,000 fine. He is the first person brought to trial under a 1986 federal computer fraud and abuse law that makes it a felony to break into a federal computer network and prevent authorized use of the system. Morris testified that he had made a programming error that caused a computer "worm" to go berserk and cripple the Internet system back on November 2, 1988. The "worm" he designed immobilized an estimated 6,000 computers linked to Internet, including ones at the NASA, some military facilities and a few major universities. Morris's attorney Thomas Guidoboni argued that Morris never intended to prevent authorized access. However testimony showed Morris did indeed deliberately steal computer passwords from hundreds of people so the "worm" could break into as many computers as possible. It was brought out in the trial that he took deliberate and conscious steps to make the rogue program difficult to detect and eliminate. Morris camouflaged sending of the program by unleashing it from the computer system at Massachusetts Institute of Technology in Cambridge and made it look like it had been sent from the University of California at Berkeley so authorship of the program could not be traced to him at Cornell. Other evidences showed Morris had at least six earlier versions of the "worm", which had been found on his Cornell computer accounts and that his own comments on the "worm" program used the words "break-in" and "steal".

---

**✦ Advance Program for Oakland Symposium (REVISED, 9 Jan 90)**

Debbie Cooper <cooper@sm.unisys.com>

Mon, 15 Jan 90 10:34:30 PST

1990 IEEE Symposium on Research in Security and Privacy  
ADVANCE PROGRAM (Proceedings later from IEEE)  
Monday, May 7, 1990

Praxis I, Steve Lipner, Chair  
Status Update, Steve Lipner  
A VMM Security Kernel for the VAX Architecture, Paul Karger, Mary Ellen  
Zurko, Douglas W. Bonin, Andrew H. Mason  
An Architecture for Practical Delegation in a Distributed System, Morrie  
Gasser, Ellen McDermott  
Practical Authentication for Distributed Computing, John Linn  
SP3 Peer Entity Identification, Bill Birnbaum

Praxis II, Elizabeth Sullivan, Chair  
The Army Secure Operating System, Neil Waldhart  
Specification and Verification of the ASOS Kernel, Ben L. Di Vito,  
Paul H. Palmquist, Eric R. Anderson, Michael L. Johnston

Database I, Teresa Lunt, Chair  
Integrating an Object-Oriented Data Model with Multilevel Security,  
Sushil Jajodia, Boris Kogan  
A Little Knowledge Goes a Long Way: Fast Detection of Compromised Data  
in 2-D Tables, Dan Gusfield  
Extending the Brewer-Nash Model to a Multilevel Context, Catherine Meadows

Database II, Earl Boebert, Chair  
Polyinstantiation and Integrity in Multilevel Relations, Sushil Jajodia,  
Ravi Sandhu  
Naming and Grouping Privileges to Simplify Security Management in Large  
Databases, Robert W. Baldwin  
Referential Secrecy, Rae K. Burns

Tuesday, May 8, 1990

Information Flow, John Rushby, Chair  
Information Flow in Nondeterministic Systems, J. Todd Wittbold, Dale M. Johnson  
Constructively Using Noninterference to Analyze Systems, Todd Fine  
Probabilistic Interference, James W. Gray, III  
Security Models and Information Flow, John McLean

Access Control and Integrity, Roger Schell, Chair  
Beyond the Pale of MAC and DAC -- Defining New Forms of Access Control,  
Catherine Jensen McCollum, Judith R. Messing, LouAnna Notargiacomo  
Some Conundrums Concerning Separation of Duty, Michael J. Nash, Keith R. Poland

Authentication, Tom Berson, Chair

The Role of Trust in Protected Mail, Martha Branstad, W. Curtis Barker,  
Pamela Cochrane

On the Formal Specification and Verification of a Multiparty  
Session Protocol, Pau-Chen Cheng, Virgil D. Gligor

Reasoning about Belief in Cryptographic Protocols, Li Gong, Roger Needham,  
Raphael Yahalom

A Security Architecture and Mechanism for Data Confidentiality  
in TCP/IP Protocols, Raju Ramaswamy

Auditing and Intrusion Detection, Jim Anderson, Chair

The Auditing Facility for a VMM Security Kernel, Kenneth F. Seiden,  
Jeffrey P. Melanson

Adaptive Real-time Anomaly Detection Using Inductively Generated  
Sequential Patterns, Henry S. Teng, Kaihu Chen, Stephen C-Y Lu

Auditing the Use of Covert Storage Channels in Secure Systems, Shih-Pyng  
Shieh, Virgil D. Gligor

Wednesday, May 9, 1990

Verification, Deborah Cooper, Chair

The Deductive Theory Manager: A Knowledge Based System for Formal Verification,

Ben Di Vito, Cristi Garvey, Davis Kwong, Alex Murray, Jane Solomon, AmyWu

Formal Construction of Provably Secure Systems with Cartesian, Heinz

Brix, Albert Dietl

Verifying A Hardware Security Architecture, Joshua D. Guttman, Hai-Ping Ko

A Hierarchical Methodology for Verifying Microprogrammed Microprocessors,  
Phillip Windley

Database III, Cristi Garvey, Chair

Transaction Processing in Multilevel-Secure Databases Using Replicated  
Architecture, Sushil Jajodia, Boris Kogan

Multiversion Concurrency Control for Multilevel Secure Database  
Systems, T.F. Keefe, W.T. Tsai

Modeling Security-Relevant Data Semantics, Gary W. Smith

Covert Channels Panel, Marv Schaefer, Chair

A1 With a Twist: Can a Fast Machine Be Secured?

Post-Symposium Panel Session, Carl Landwehr, Chair

International Orange II: A Spectrum of Computer Security Criteria



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 9: Issue 63

Wednesday 31 January 1990

## Contents

- [Vive la difference?](#)  
[Peter G. Neumann](#)
- [Airbus crash of June 88](#)  
[Olivier Crepin-Leblond](#)
- [AT&T Crash Statement: The Official Report](#)  
[Don H Kemp via Geoff Goodfellow](#)
- [Important Lesson from AT&T Tragedy](#)  
[Bill Murray](#)
- [Potential Lesson From AT&T](#)  
[Bill Murray](#)
- [Sun Sendmail Vulnerability](#)  
[Kenneth R. van Wyk](#)
- [GPO Library disk infection \(PC\)](#)  
[Kenneth R. van Wyk](#)
- [Re: Password Sharing](#)  
[Al Arsenault](#)
- [Annual Computer Security Applications Conference](#)  
[Marshall D. Abrams](#)
- [Virology](#)  
[Gene Spafford](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **Vive la difference?**

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

Sat, 27 Jan 1990 12:45:57 PST

WOMEN ENJOY COMPUTERS MORE THAN MEN, SURVEY SAYS

-- Rockford (Ill.) Register Star.

Yes, but can computers take out the garbage?

-- The New Yorker, 29 Jan 90, p.89.

No, but they can generate it faster.

-- PGN, 27 Jan 90.

---

## **✈ Airbus crash of June 88**

*Olivier Crepin-Leblond <zdee699@elm.cc.kcl.ac.uk>*

*Tue, 30 JAN 90 09:35:42 GMT*

On the 26th June 1988 at 12:45:39, flight ACF 296Q, an Airbus owned by the German company Durus Verwaltungsgesellschaft MBH Co Mobilien KG, and exploited by AIR FRANCE crashed in a forest in eastern France, whilst flying at very low altitude during an Air Show.

Today, the captain, Michel Asseline has lost his French pilot license for 8 years. He is now flying in Australia.

One and a half years after this accident it is still not known why this crash happened. A report written by the commission dealing with the enquiries about the crash has not yet been released to the public, but "Le Temps de la Finance", a French financial newspaper is now able to give at least SEVEN major contradictions in the report. Please note that the report they had in hand was the final draft.

Le Temps de la Finance. Nr. 59 Thursday, 18 January 1990.

" The first part of the conclusions implicates the organisers of the air show and the company AIR FRANCE. The planning of the flight was insufficient because the whole file was submitted too late. The commission doing the enquiry revealed that the technical flight plan given to the crew of the aircraft by the regional operations department of AIR FRANCE did not mention anything about the axis of the runway, or the altitude of the flight.

One of our informers pointed-out that the different flight plans given to the commission, including messages to/from the crew were bad quality photocopies.

The airport on which the tragedy happened had 2 parallel runways which were not fit to receive an A320 should an incident occur."

There then follows a reminder that this was a demonstration flight and the passengers were in a very joyful mood. One argues that this could have been transmitted to the pilots. The aircraft was one of a new type which might have triggered an excess of confidence in the pilot's head. In addition, the size of the airport was so small that the pilot might have thought he was at a higher altitude.

" The commission has implied NO FAULT concerning the functioning of the aircraft, or its design. However, certain affirmations of the commission leading the enquiry can be discussed...

1: On the day of the accident, the altimeter reference value had been changed to a value which was not sensible. The commission emphasizes that since that time, it has never happened again. But an aeronautical specialist has confirmed to us that it is impossible to affirm that this anomaly has never happened since.

2: when the DFDR (Digital Flight Data Recorder) (A Fairchild 800) was decoded,

some of the data was badly restituted. During 8 seconds, the readings of the data were incorrect and corrupted, and some errors in the software controlling the restitution of parameters of the A320 are thought to be the cause of the anomaly, the report says. The tape was therefore cleaned and then most of the data was read without problems. But the examining magistrate is now talking about verifying the authenticity and integrity of the flight recorder data.

3: The commission noted that the data of the DFDR is incoherent for 3 seconds starting 12:45:39, which is the exact time of the crash, and then data relating to an earlier flight is found since the DFDR functions in a closed loop. But a specialist told us that this is technically impossible !

This view agrees with information published in [another French newspaper], the "Canard Enchaîné" on Wednesday 17 January 89 which was talking about irregularities and interference concerning the DFDR decoding. That paper disclosed that the tape was cut and information transferred to another tape for reading and decoding...

4: The emergency lighting did not work because of a programming error. (this information is repeated twice in the report, pages 28 and 31). In aeronautical circles, it is said that this is 'due to a bad power supply which was corrected in many months because of problems concerning the official approval' [ !? ]. The organisation which certified the circuit, the DGAC (Direction Generale de l'Aviation Civile [ French equivalent of FAA - ocl]) is a branch of the same organisation which controls the IGAC, the commission which led the enquiry.

The signal requesting evacuation of the cabin did not apparently work since nobody heard it, and the head of the cabin crew did not manage to find the microphone of the public address system. It had apparently broken-off from its stand, which was very fragile.

5: Did the equipment broadcasting the altitude work all right ? (this is a hypothesis). It was heard at 100 feet. But then the dialogue between the pilots was interrupted and from that time nothing is really sure.

The pilot told the control tower that he was at 100 feet, and flight plans indicate a minimum of 100 feet, but it was observed from the ground that the aircraft was in fact at 30 feet. On page 55 of the report, it is said that if the airplane drops under the required altitude, this implies that the captain is piloting by sight, and has not registered the data given by the vocal equipment. But Michel Asseline cut-out the automatic protection for thrust (Alpha-floor). This is needed when there is a need to fly over 100 feet and the aircraft is very inclined. But why would he cut it out when flying under 100 feet, since it is automatically de-activated under that altitude ?

And then there is also the surprise of the pilots in the cockpit when the airbus chopped the first trees of the forest: 'Shit, the trees !'

This tends to prove that the pilots were not aware of their low altitude, and that they were not aware of the presence of this patch of forest, since it was not marked on the plan, although electric pylons are noted 1.5Km away from that zone.

[...]

... all of these deficiencies seem to accumulate, on an aircraft which, according to the commission had NO MECHANICAL AND INSTRUMENTAL DEFICIENCY WHICH COULD ENDANGER THE AIRCRAFT'S SAFETY.

6: Did the engines work properly ? As soon as he escaped from the aircraft, the captain Michel Asseline cast doubts on the response of the engines. These are built by CFM, a 50/50 between General Electric (USA) and Snecma (France)."

There then follows a number of contradictory statements from Snecma and Asseline, and the fact that one can feel that an engine is not giving enough power to 'leap-out' of such a situation under these circumstances, since the engines cannot instantaneously give maximum thrust.

" Asseline answers that the constructors of the engine CFM56 were aware of the problems of acceleration of the engine at low altitude but told AIR FRANCE about that only after the crash."

Along with the article is a photocopy of a bulletin released by Airbus Industrie Flight Division, entitled:

"Operations Engineering Bulleting - A320.  
Validity A320 - CFM only  
Bulletin Nr. 19/1 DATE: MAY 88

Reasons for issue:

It has been observed (recently), so far on test aircraft only, that a VSV position control deficiency could prevent the engines from accelerating up to full power under certain flight conditions:

- low altitude
- high aircraft speed
- engine acceleration initiated from N1 between 40% and 70%

Two production aircraft have been checked and no engine presented any sign of this problem.

Explanation:

[...]

The most likely reason for the problem is a lack of muscle pressure to control the VSV's to their intended position when aerodynamic loads are high. Therefore the problem is unlikely to occur at low aircraft speed.

Actions:

A full investigation... [...]

As a precautionary measure, the following procedure it to be applied should the problem be encountered.

Procedures:

If the "compressor vane fault" warning come-on ECAM at low altitude (below 10000 feet), associated with a lack of N1 response (typical values for throttle position: 100% N2, 80% N1), the fault can be cleared by decelerating the engine to idle, and then performing a rapid acceleration from idle speed to full power. "

The newspaper says that 2 conditions out of 3 were met, and that the engine throttle positions were the same during the crash. N1 is low power throttle position (40% - Max 80%). One second before the crash , N1 was 67%. It then increased to 83% and 84%. A failure was possible. Since the aircraft serial number was 009, it could be considered as nearly being still a prototype.

"7: The report is incoherent on a few points. It doesn't get alarmed that although the stick was pulled back fully (written on pages 22 and 43), the inclination of the Airbus did not change.

[...]

Last problem: Can the DGAC, through the commission leading the enquiry, admit that an aircraft that it certified earlier is deficient ?

All parties involved, Air France, the French Civil Aviation Authority, the Snecma, are all owned or controlled by the French State.

Would the French State have any advantage in taking itself to court ?"

There then follows a discussion about the political and economic factors at stake. Enormous sources of revenue from exportation of Airbus and of CFM56 engines which also equip some Boeing aircraft.

The article concludes that if nothing was wrong with the aircraft, it is in everybody's interest to help the inquiry so that all questions that remain can be answered, and the public be hopefully reassured why the flight ACF 296 Q terminated in the woods of Hasheim, in the east of France.

disclaimer: I know, I am a hopeless translator. I am merely relaying to this list what I read in the paper. I have no opinion on that matter, neither does KCL or in fact anyone I know... So please: no flames, thanks.

Olivier Crepin-Leblond, Computer Systems & Electronics Eng.  
Electrical & Electronic Eng., King's College London, UK.

---

## **✂ Re: AT&T Crash Statement: The Official Report**

*Geoff Goodfellow <geoff@fernwood.mpk.ca.us>*

*Mon, 29 Jan 90 19:47:42 -0800*

>Date: 28 Jan 90 17:24:48 GMT

>From: dhk@teletech.uucp (Don H Kemp)

>Newsgroups: comp.dcom.telecom

>Subject: AT&T Crash Statement: The Official Report

>Organization: TELECOM Digest

Here's AT&T's \_official\_ report on the Martin Luther King day network problems, courtesy of the AT&T Consultant Liason Program.

Don

=====

Technical background on AT&T's network slowdown, January 15, 1990

\* \* \*

At approximately 2:30 p.m. EST on Monday, January 15, one of AT&T's 4ESS toll switching systems in New York City experienced a minor hardware problem which activated normal fault recovery routines within the switch. This required the switch to briefly suspend new call processing until it completed its fault recovery action -- a four-to-six second procedure. Such a suspension is a typical maintenance procedure, and is normally invisible to the calling public.

As part of our network management procedures, messages were automatically sent to connecting 4ESS switches requesting that no new calls be sent to this New York switch during this routine recovery interval. The switches receiving this message made a notation in their programs to show that the New York switch was temporarily out of service.

When the New York switch in question was ready to resume call processing a few seconds later, it sent out call attempts (known as IAMs - Initial Address Messages) to its connecting switches. When these switches started seeing call attempts from New York, they started making adjustments to their programs to recognize that New York was once again up-and-running, and therefore able to receive new calls.

A processor in the 4ESS switch which links that switch to the CCS7 network holds the status information mentioned above. When this processor (called a Direct Link Node, or DLN) in a connecting switch received the first call attempt (IAM) from the previously out-of-service New York switch, it initiated a process to update its status map. As the result of a software flaw, this DLN processor was left vulnerable to disruption for several seconds. During this vulnerable time, the receipt of two call attempts from the New York switch -- within an interval of 1/100th of a second -- caused some data to become damaged. The DLN processor was then taken out of service to be reinitialized.

Since the DLN processor is duplicated, its mate took over the traffic load. However, a second couplet of closely spaced new call messages from the New York 4ESS switch hit the mate processor during the vulnerable period, causing it to be removed from service and temporarily isolating the switch from the CCS7 signaling network. The effect cascaded through the network as DLN processors in other switches similarly went out of service. The unstable condition continued because of the random nature of the failures and the constant pressure of the traffic load in the network providing the call-message triggers.

The software flaw was inadvertently introduced into all the 4ESS switches in the AT&T network as part of a mid-December software update. This update was intended to significantly improve the network's performance by making it possible for switching systems to access a backup signaling network more quickly in case of problems with the main CCS7 signaling network. While the software had been rigorously tested in laboratory environments before it was introduced, the unique combination of events that led to this problem couldn't be predicted.

To troubleshoot the problem, AT&T engineers first tried an array of standard procedures to reestablish the integrity of the signaling network. In the past, these have been more than adequate to regain call processing. In this case,

they proved inadequate. So we knew very early on we had a problem we'd never seen before.

At the same time, we were looking at the pattern of error messages and trying to understand what they were telling us about this condition. We have a technical support facility that deals with network problems, and they became involved immediately. Bell Labs people in Illinois, Ohio and New Jersey joined in moments later. Since we didn't understand the mechanism we were dealing with, we had to infer what was happening by looking at the signaling messages that were being passed, as well as looking at individual switches. We were able to stabilize the network by temporarily suspending signaling traffic on our backup links, which helped cut the load of messages to the affected DLN processors. At 11:30 p.m. EST on Monday, we had the last link in the network cleared.

On Tuesday, we took the faulty program update out of the switches and temporarily switched back to the previous program. We then started examining the faulty program with a fine-toothed comb, found the suspicious software, took it into the laboratory, and were able to reproduce the problem. We have since corrected the flaw, tested the change and restored the backup signaling links.

We believe the software design, development and testing processes we use are based on solid, quality foundations. All future releases of software will continue to be rigorously tested. We will use the experience we've gained through this problem to further improve our procedures.

It is important to note that Monday's calling volume was not unusual; in fact, it was less than a normal Monday, and the network handled normal loads on previous weekdays. Although nothing can be guaranteed 100% of the time, what happened Monday was a series of events that had never occurred before. With ongoing improvements to our design and delivery processes, we will continue to drive the probability of this type of incident occurring towards zero.

Don H Kemp, B B & K Associates, Inc., Rutland, VT uunet!uvm-gen!teletech!dhk

---

### **✂ Important Lesson from AT&T Tragedy**

<WHMurray.Catwalk@DOCKMASTER.NCSC.MIL>  
Sun, 28 Jan 90 10:00 EST

[A tragedy is when you learn the wrong thing from a fiasco.]

After AT&T's early and re-assuring statements about the nature of their recent failure, I complained about the potential to permanently mislead their employees about the nature of the failure. Now it turns out that the statements were premature and misleading.

I comment now at the risk of still being too soon. However, I will limit my comments to the community and to what is now already all too clear.

THE FAILURE WAS NOT IN THE FAILURE OF A SINGLE PIECE OF SOFTWARE.

NEITHER IS IT LIKELY TO BE AN ISOLATED CONDITION.

The failure was not, as was first suggested, a propagating alarm condition. Rather, IT WAS THE INABILITY TO PROPERLY HANDLE THE RETURN TO THE LINE OF A FAILING COMPONENT. It was not a COMPONENT problem; it was, as I feared and suggested a SYSTEM problem. This is a growing class of complex system failure.

It was the major cause of the NASDAQ outage and it contributed to Hinsdale. NASDAQ's system behaved as expected when the service from the local utility dropped. It failed when the external power came back on line. The ability of the operator in down-state Illinois to properly read the situation in Hinsdale was complicated by the fact that the power system and the fire alarms were coupled, in a subtle way, so as to confuse the readings, and because the attempts of automatic systems to compensate for the fire, not only perpetuated the fire, but confused the alarm information even further.

We are testing to see what happens when a component fails. WE ARE NOT PROPERLY TESTING TO SEE WHAT HAPPENS WHEN THE COMPONENT SUCCEEDS IN CORRECTING ITSELF AND COMES BACK ON LINE.

William Hugh Murray, Fellow, Information System Security, Ernst & Young  
2000 National City Center Cleveland, Ohio 44114  
21 Locust Avenue, Suite 2D, New Canaan, Connecticut 06840

---

### **✂ Potential Lesson From AT&T**

<WHMurray.Catwalk@DOCKMASTER.NCSC.MIL>  
Sun, 28 Jan 90 10:17 EST

Potentially, there is a second lesson to be learned from AT&T. It is that it is possible to over-automate. As I noted earlier, the real problem was not that a component failed, but that the system could not tolerate it coming back on-line.

Note that AT&T had automated the procedure for restoring a failing component. This decision contributed to the failure. Now, if this kind of component failure was so common that manual intervention would be ineffective and inefficient, then the decision to automate it would be appropriate. Otherwise, it is an example of OVER AUTOMATION. Such automation adds so much complexity that it causes failures that would not have taken place in its absence.

AUTOMATE ONLY THOSE THINGS THAT HAPPEN WITH SUFFICIENT FREQUENCY THAT AUTOMATION IS JUSTIFIED. AVOID GRATUITOUS AUTOMATION.

Notice that the procedure was inadequately tested, and that this contributed to the failure. In fairness to AT&T and others who have had similar problems, such conditions are difficult to simulate and the procedures difficult to test.

IF YOU CANNOT TEST IT, DO NOT DO IT.

William Hugh Murray, Fellow, Information System Security, Ernst & Young  
2000 National City Center Cleveland, Ohio 44114

21 Locust Avenue, Suite 2D, New Canaan, Connecticut 06840

---

## **Sun Sendmail Vulnerability**

*Kenneth R. van Wyk <krvw@SEI.CMU.EDU>*

*Mon, 29 Jan 90 16:47:21 EST*

CERT Advisory  
29 January 1990  
Sun Sendmail Vulnerability

The Computer Emergency Response Team Coordination Center (CERT/CC) has learned of, and has verified, break-ins on several Internet systems in which the intruders have exploited a vulnerability in the Sun sendmail program. This vulnerability exists in all versions of SunOS up to and including the current version, 4.0.3 on Sun 3, Sun 4, and Sun 386i systems (note that 4.0.2 is the most current version of SunOS on the 386i machines). That is, all current Sun systems.

The vulnerability has previously been reported to Sun and a solution to this problem (Sun bug # 1028173) is available via a new version of sendmail supplied by Sun. The new sendmail is available directly from the Sun Answer Center (1-800-USA-4SUN). Sun 3 and Sun 4 sendmail binaries are also available via anonymous FTP from uunet.uu.net in the /sun-fixes directory.

This incident underscores the need for system administrators to maintain an awareness of the steps their vendors are taking to improve the security aspects of their products, and to seriously consider upgrading system configurations when solutions to security problems are made available.

Administrators of Sun systems are urged to contact Sun for the new version of the sendmail program. Administrators of machines other than Suns are urged to contact their vendors to verify that they are running the latest version of sendmail, since there may have been security related fixes to it in the past year.

If you need further information on this problem, contact your Sun representative or CERT/CC. CERT/CC can be contacted by telephone at (412) 268-7090 (24 hours) or email to cert@cert.sei.cmu.edu (monitored daily).

Our thanks to Matt Bishop and Wayne Cripps for their efforts in analyzing and investigating this problem and its solution.

Kenneth R. van Wyk, Technical Coordinator, Computer Emergency Response Team  
Software Engineering Institute, Carnegie Mellon University  
cert@CERT.SEI.CMU.EDU (412) 268-7090 (24 hour hotline)

[Perhaps the "secure" version would fix the RISKS sendmail timeout problem that occasionally gives some of you multiple copies of RISKS, but then there apparently are other things that we need that it does not do! For this reason there are various versions of sendmail floating around, none of which is quite what is needed. Oh, well, what's new? PGN]

---

## **✂ GPO Library disk infection (PC)**

*Kenneth R. van Wyk <krvw@SEI.CMU.EDU>*

*30 Jan 90 19:29:04 GMT*

I phoned the folks at the GPO and confirmed that the above report is indeed true. They faxed me a copy of a letter which they're sending out to the people that they know have received the disks. Below is a (transcribed - sorry if there are typos) copy of that fax.

Ken

===== Cut Here =====

Dear Depository Librarian:

GPO has just been notified by the Census Bureau that one of the floppy disks just distributed by GPO with the \_County and City Data Book\_ CD-ROM is infected with a computer virus AND SHOULD NOT BE USED UNDER ANY CIRCUMSTANCES. The floppy disk was listed on shipping list 90-0057-P as C 3.134/2:C 83/2/988/floppy-2. The title on the floppy disk reads as follows:

Bureau of the Census  
Elec. County & City Data Bk., 1988  
U.S. Stats., Inc., 1101 King St.,  
Suite 601, Alexandria, VA 22314  
(703) 979-9699

PLEASE DESTROY THE FLOPPY DISK AS SOON AS IT IS RECEIVED. (Do NOT reformat and reuse the floppy disk.)

The virus has been identified as the Jerusalem-B virus (also referred to as the Israeli virus). It infects any .COM or .EXE program on MS-DOS personal computers and increases program size by approximately 1,800 bytes. Other programs are infected when they are executed in an infected system.

The Jerusalem virus can cause significant damage on an infected personal computer. It generally slows down the system and some versions destroy all data on the hard disk. .EXE files continue to grow in size until they are too large to execute.

If your computer has already been infected, we recommend that, if possible, you seek assistance from a computer specialist at your institution immediately. There are special programs available for detecting and eradicating computer viruses. One may be available in your institution or from someone you know. DO NOT USE YOUR PC TO ACCESS A NETWORK OR PRODUCE FLOPPY DISKS CONTAINING .EXE OR .COM PROGRAMS FOR BY OTHER PCS.

The \_County and City Data Book\_ CD-ROM can be used safely with the software on the other floppy disk distributed in that shipment ((C 134/2:C 83/2/988/floppy).

If you have any questions, please call Jan Erickson at GPO (202 275-1003) or the Census Bureau Customer Service at (301 763-4100).

The Census Bureau and GPO regret any problems that this may have caused. Appropriate measures will be taken to ensure that it does not happen again.

---

**✉ Re: Password Sharing [Arsenault, [RISKS-9.57](#)]**

*Al Arsenault <AArsenault@DOCKMASTER.NCSC.MIL>  
Tue, 30 Jan 90 12:31 EST*

In response to the many comments regarding my previous transaction, about the student who responded to a test question that passwords are better than biometrics because one can give out a password to a friend and thus does not need to be physically present when the friend logs in to one's account:

I gave the student no credit for his answer. (It made no difference whatsoever in his semester grade.) True, I could have worded the question differently: "If one is concerned about maintaining individual accountability, what is one advantage...". However, I did not believe that the lack of the qualifier made his answer acceptable: the student should have understood the context of the question.

In discussing the question/answer with the student afterward, I described a situation that happened a couple of years ago in another class I was teaching. (The story is true; the names have been changed to protect the guilty.)

I was teaching a course in Pascal programming to a class of Information Systems Management majors. "Joe", a student in the class, was engaged to "Sue", who had taken the course the previous semester. Joe told Sue his password, so that she could help him with his class programming assignments. However, in the middle of the semester, Joe dumped Sue for Sally, another student in the current class.

For Sue, revenge was sweet. Since she knew Joe's password, she logged in to his account and 'fixed' his programs. She didn't delete his files; that would have been obvious, and fixable from backup tapes. Instead, she subtly changed lines of code in the programs (e.g., 'while (x < MaxSize)...' became 'while (x<= MaxSize)...'). The net result was that the programs ran, but gave incorrect answers.

Joe never did find out what happened. I found out about it because Joe wound up failing the class (NOT just because the programs didn't work, but that contributed). Sue felt guilty; she came to see me after the semester and explained what she had done. I made some comment to her about 'he should have changed his password after changing his personal life'. She said that he eventually did. But, Joe told his new password to three or four of his other friends; it was not difficult for her to find out his new password from one of them.

As I explained to the Computer Security student, this is exactly the problem with sharing your password. Once you have given it to someone else, you have lost control of it. There is no real way of being sure exactly who knows your password and what is being done with/to your account, unless you can completely trust everyone you give your password to.

Now, I do understand that sometimes individual accountability is not important. If the security policy for the system says that individual accountability is not an issue, and everyone clearly understands what that means, then I have no problems with sharing passwords. I just want everyone to understand the potential consequences before they make that decision.

I also understand that, no matter what security policies/rules say, some people are going to do what they want - including sharing passwords, etc. I cannot stop that, any more than I can stop people from breaking other rules/laws, etc. As a teacher, what I want to do is make people aware of the possible consequences of breaking those rules. That applies to the consequences from the Academic Computing Center ("we're terminating this account, because you didn't abide by the rules") and to the consequences from those who get access to the accounts. Once users understand the rules, the reasons, and the consequences, they will make their own decisions. The only thing I can do is report anything I personally know about to appropriate authorities, and hope for the best with the rest.

(To further someone's analogy about giving someone your ATM card and PIN when you're ill, so they can get you some money: understand before you do it that, if this person wants to take some extra money from your account and pocket it, (s)he can. If this person loses your card and the slip of paper (s)he has written the PIN on, then someone else can get your money. Once you understand that, then you have to make up your own mind about whether the risk is worth the benefit.)

Al Arsenault

---

## **✉ Call for papers: Annual Computer Security Applications Conference**

*(Marshall D. Abrams) <abrams@soldier.mitre.org>*

*Wed, 31 Jan 90 09:05:43 -0500*

### **CALL FOR PAPERS AND PARTICIPATION**

**Sixth Annual Computer Security**

**Applications Conference**

**December 3-7, 1990**

**Tucson, Arizona**

### **The Conference**

Operational requirements for civil, military, and commercial systems increasingly stress the necessity for information to be readily accessible. The Computer Security Act of 1987 requires that all Federal agencies take certain actions to improve the security and privacy provided by federal computer systems. Accomplishing both operational and security requirements

requires the application of the maturing technology of integrated information security to new and existing systems throughout their life cycle.

This conference will explore technology applications for both civil and military systems; the hardware and software tools and techniques being developed to satisfy system requirements; and specific examples of systems applications and implementations. Security policy issues and standards will also be covered during this five day conference.

#### Papers, Tutorials, and Vendor Exhibits

Technical papers and tutorials that address the application of integrated information security technologies in the civil, defense, and commercial environments are solicited. Original research, analyses and approaches for defining the computer security issues and problems identified in the Conference's interest areas; secure systems in use or development; methodological approaches for analyzing the scope and nature of integrated information security issues; and potential solutions are of particular interest. We are also interested in vendor presentations of state-of-the-art information security products.

#### INSTRUCTIONS TO AUTHORS:

Send five copies of your paper or panel proposal to Dr. Ronald Gove, Program Chairman, at the address given below. Tutorial proposals should be sent to Dr. Dixie Baker at the address given below. We provide "blind" refereeing; put names and affiliations of authors on a separate cover page only. It is a condition of acceptance that manuscripts submitted have not been published. Papers that have been accepted for presentation at other conferences should not be submitted.

Papers and tutorial proposals must be received by May 18, 1990. Authors will be required to certify prior to June 20, 1990, that any and all necessary clearances for publication have been obtained, that they will attend the conference to deliver the paper, and that the paper has not been accepted elsewhere. Authors will be notified of acceptance by July 30, 1990. Camera ready copies are due not later than September 19, 1990. Material should be sent to:

Dr. Ronald A. Gove	Dr. Dixie B. Baker
Technical Program Chair	Tutorial Program Chair
Booz-Allen & Hamilton Inc.	The Aerospace Corporation
4330 East-West Highway	P.O. Box 92957, MI/005
Bethesda, MD 20814	Los Angeles, CA 90009
(301) 951-2395	(213) 336-7998
Gove@dockmaster.ncsc.mil	baker@aerospace.aero.org

#### Areas of Interest Include:

GOSIP C3I Systems  
ISO/OSI Security Architecture Policy and Management Issues  
Advanced Architectures SDNS  
Trusted DBMSs and Operating Risk/Threat Assessments  
Systems Network Security  
Public Law 100-235 Medical Records Security  
Current and Future Trusted State-of-the-Art

System Technology      Trusted Products  
Space Station Requirements      Certification, Evaluation, and  
   Accreditation

Reviewers and Prospective Conference Committee Members

Anyone interested in participating as a reviewer of the submitted papers, please contact Dr. Ron Gove at the address given above. Those interested in becoming members of the conference committee should contact Dr. Marshall Abrams at the address below.

Additional Information

For more information or to receive future mailings, please contact the following at:

The MITRE Corporation      Marshall Abrams  
7525 Colshire Drive Conference Chairman  
McLean, VA 22102      (703) 883-6938  
   abrams@mitre.org

Diana Akers or Victoria Ashby  
Publicity and Publication Chairs  
(703) 883-5907 or (703) 883-6368  
akers%smiley@gateway.mitre.org  
ashby%smiley@gateway.mitre.org

---

## Virology

*Gene Spafford <spaf@cs.purdue.edu>*  
*Mon, 29 Jan 90 11:01:17 EST*

"Computer Viruses: Dealing with Electronic Vandalism and Programmed Threats" by Eugene Spafford, Kathleen Heaphy, and David Ferbrache. 1989, 109 pages. Published by ADAPSO.

The book has been written to be an accessible resource guide for computer users and managers (PC and mainframe). It presents a high-level discussion of computer viruses, explaining how they work, who writes them, and what they do. It is not intended to serve as a technical reference on viruses, both because the audience for such a work would be limited, and because such a reference might serve to aid potential virus authors.

The goal of the book is to dispell some common myths about viruses (and worms, trojan horses, et. al.), and provide simple, effective suggestions for how to protect computer systems against these threats. It furthermore stresses that most systems face greater threats from other areas, so the proper attitude to take is to strengthen overall security; concrete suggestions for enhancing overall security are also presented.

The appendices provide extensive references to other publications, security organizations, anti-viral software sources, applicable (U.S.) state and

Federal laws against computer crime, and detailed descriptions of all IBM and Apple Macintosh viruses known as of 1 October 1990.

Although written for ADAPSO members, almost any computer user should find it instructive. The appendices are an excellent source of further information, addresses and phone numbers, and pointers to software. At least one university professor has indicated he will use the book in a security course, and some law enforcement agencies are also considering using the book for instructional purposes.

The authors are interested in comments and feedback about the book, especially in areas where information might be added. You can contact them by sending mail to "virus-book@cs.purdue.edu"

Table of Contents: Preface, Executive Summary, Introduction, Programmed Threats, What is a Computer Virus?, Names, Dealing with Viruses, Prevention, Security, Legal Issues, Attitudes, Further Information on Viruses, Information on Anti-Viral Software, Further Information on Legal Aspects of Viruses, Further Reading and Resources

A copy can be ordered from ADAPSO, 1300 North Seventeenth St., Suite 300, Arlington, VA 22209 USA, Attn: Mr. John Gracza. Single copies are \$30. Copies ordered on university stationary or on stationary of ADAPSO member companies is only \$20, and \$16 for the second and subsequent copies. Requests for review copies or special considerations should be addressed directly to John Gracza. Copies have been given away to ADAPSO member companies, and various state and Federal law enforcement agencies, so check with others in your organization to see if a copy isn't already available for review. Overseas orders will be shipped surface mail. Overseas air mail \$10 extra.



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 9: Issue 64

Thursday 1 February 1990

## Contents

- [SENDMAIL horrors](#)  
[PGN](#)
- [Software error at Bruce nuclear station](#)  
[Mark Bartelt](#)
- [New South Wales Police deregisters police cars](#)  
[Diomidis Spinellis](#)
- [Fire and 753 controllers \(need a light?\)](#)  
[Neal Immega via Mark Seiden](#)
- [The substantiative error made by AT&T](#)  
[Robert Ullmann](#)
- [Re: AT&T Crash Statement: The Official Report](#)  
[Bob Munck](#)
- [Re: Airbus crash of June 88](#)  
[Robert Dorsett](#)
- [Re: Virology and an infectious date syndrome](#)  
[Gene Spafford](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✉ SENDMAIL horrors

*Really from Neumann@csl.sri.com <RISKS Forum <risks@csl.sri.com>>  
Thu, 1 Feb 1990 10:59:38 PST*

My sincerest apologies to those of you who received multiple copies of [RISKS-9.63](#). I keep breaking the mailing list up into smaller sublists, but for the first time TWO of the sublists were victimized by the lurking SENDMAIL flaw. I will try mailing this issue to the sublists sequentially, waiting for each sublist to complete before going on to the next, just in case there are competing effects. I have been putting out fewer issues in hopes of minimizing your annoyance, but that is also counterproductive. So, please bear with me as I try this issue serially over the sublists... Painful, but it might help!

By the way, the end of the AT&T "Official report" message in [RISKS-9.63](#) had a few trailing blank characters that overflowed the line and made the next line

look blank on my screen, which means that the undigestifiers probably gagged on it and refused to recognize the following message separately. I try hard to avoid that, but this one slipped through. For those of you who get RISKS as individual messages, Oops. Sorry. :-(

PGN

---

## **✂ Software error at Bruce nuclear station**

*Mark Bartelt <mark@sickkids.toronto.edu>*

*Thu, 1 Feb 90 06:32:11 EST*

Mark Bartelt, Hospital for Sick Children, Toronto mark@sickkids.utoronto.ca  
416/598-6442 UUCP: {utzoo,decvax}!sickkids!mark

Group questions software's reliability after Bruce Accident  
(Canadian Press)

A computer software error that released thousands of litres of radioactive water at the Bruce nuclear station raises questions about the reliability of software at the new Darlington station, Energy Probe says. "This spurious software accident at Bruce Unit 4 should be regarded as a warning about software safety in general," Tom Adams, utility analyst with the energy watchdog group, said yesterday. But Ontario Hydro says the group is comparing "apples to oranges."

The computers at Darlington have three backup systems that automatically shut down the reactors in certain emergencies, spokesman Dave Stevens said. The Crown utility says a software flaw caused last week's accident, when a mechanical fuelling machine was loading and unloading fuel bundles into reactor Unit 4 at the Bruce station at Kincardine, near Owen Sound. No one was injured and neither workers nor the environment were directly contaminated by the tritium-irradiated heavy water, which escaped from the reactor as steam.

Although Mr. Stevens said he did not know whether Hydro had anticipated such an accident, he said the utility had contingency plans for the release of heavy water.

A spokesman for the Atomic Energy Control Board, which regulates the safety of the nuclear industry, described the accident as "very unusual and also very significant" because of what could have happened. "It has the appearance of something that could have been worse," Zygmund Domaratzki said in a telephone interview from Ottawa. "If that fuelling machine had kept on going it would have ripped the end of that channel," allowing the fuel bundles to tumble out, Mr. Domaratzki said. With that kind of mishap, he said, "it wouldn't take much to cause widespread contamination within the reactor building." As it was, the accident cost Hydro time and money, he said.

Meanwhile, heavy water continued leaking from the Bruce reactor yesterday at the rate of about seven litres per hour. Workers planned to remove 13 fuel bundles from the damaged fuel channel and retrieve the fuelling machine, still dangling on the face of the reactor. The unit is expected to be down for at least six weeks.

Because two of the other three reactors at Bruce are still down, the giant utility may have problems meeting demand if there is a severe cold snap.

---

### **✂ New South Wales Police deregisters police cars**

*Diomidis Spinellis <dds@cc.imperial.ac.uk>*

*Tue, 30 Jan 90 12:20:55 GMT*

Found in the British "Guardian" newspaper of 25 January 1990:

"The entire state police force in the New South Wales Australia, found itself driving illegal cars after an enthusiastic computer deregistered them, Paul Zucker reports on the Newsbytes online newsletter. The police were instructed to book themselves, or each other.

"The problem was cause by a high ranking officer (not named) who failed to pay illegal parking tickets. His unmarked car was registered to the police department. After statutory warnings were ignored, the computer program deregistered all cars belonging to the offender: that is, all cars belonging to the police department."

It may be that I am still under the influence of Dijkstra's CACM article, but notice how the computer is given the human attribute "enthusiastic".

Diomidis Spinellis, Imperial College, London.

---

### **✂ Fire and 753 controllers (need a light?)**

*Mark Seiden <mis@Seiden.com>*

*Wed, 31 Jan 90 21:39:22 EST*

posted recently (edited slightly):

Subject: Fire and 753 controllers

Date: 30 Jan 90 14:25:25 GMT

[From: Neal Immega]

Organization: Shell Development Company, Bellaire Research Center, Houston, TX

Shell Development Co. had a fire in a SUN 4/280 when diodes on a Xylogics 753 disk controller overheated and caught fire. The plastic card guides on the Illmanite double wide to triple wide controller also appear to have burned and may have contributed to the damage of the two adjacent disk controller cards (which operated perfectly while burning!). Flames four inches high were coming out of the top of the card cage when the fire was extinguished.

This problem could have been prevented if we had been notified of the 10/10/89 field change notice from Xylogics to make a free upgrade to all boards by adding a heatsink for the diodes. The new design has a bronze colored strip 1.5 inch wide running the length of the card.

Xylogics said that I should have been notified by the distributor (CITA Technologies) and CITA says that they were not told of the problem. The Xylogics contact for this is Laurie Walker at 617-272-8140. She will need the serial number from the board (X plus 7 numbers from the back).

Neal Immega  
Staff Geologist , Geology Research  
Shell Development Company, Bellaire Research Center (713) 663-2572  
...!rice!shell!immega immega@shell.com

[This raises the interesting question how us poor users at the bottom of the food chain are expected to find out about safety-related problems....  
Mark Seiden, mis@seiden.com, 203 329 2722]

---

### **✂ the substantiative error made by AT&T**

*Robert Ullmann <Ariel@RELAY.PRIME.COM>  
31 Jan 90 22:04:49 EST*

I am surprised that no one has pointed to the [IMHO] real error committed by AT&T: that is, upgrading all of the ESS4s to the same s/w revision at the same time.

This exposes the network to a single error, with consequences that affect the entire network simultaneously.

To contrast, from personal experience: I run the internal mail network in Prime Computer, which runs SMTP mail on 3000 systems in 27 countries. I have been criticized for not being aggressive in upgrading the revision of PDNmail (an RFC1090 implementation) to current release.

My reason is that the network is much more robust running a range of different versions (much like Long-Lines was, before everything was ESSn, with DLL'd s/w: which is why this didn't happen before). Many of the systems run other software implementations entirely, which also helps. Except when those implementations are "ports" of the same software, witness the continuing generic sendmail problems. Not that anything is wrong with sendmail, per se, but there ought to be more independent implementations-from-specification.

The resulting heterogenous network of systems is so robust that I can test new implmentations of PDNmail by replacing the mailer on the most heavily loaded system (!), and watching closely for several hours. (Not that I am generally advocating this sort of thing! "ah, Schickelgruber, you have a new version of the master S/W? It compiles, Ja? Sehr gut, load it on Hinsdale ... " :-)

Systemic problems with new versions become apparent after only a few systems are using it in production service; and only affect a small part of the network, even if undiagnosed or uncorrected for long periods of time.

Robert Ullmann, Prime Computer, Inc.

---

**✂ Re: AT&T Crash Statement: The Official Report**

*Bob Munck <munck@community-chest.mitre.org>*

*Thu, 01 Feb 90 13:43:02 -0500*

>From Telecom-Digest: Volume 10, Issue 59 and Risks Digest: 9.63

> Here's AT&T's \_official\_ report on the Martin Luther King day network

> problems, courtesy of the AT&T Consultant Liason Program.

> ...

> While the software had been rigorously tested in laboratory

> environments before it was introduced, the unique combination of

> events that led to this problem couldn't be predicted.

^^^^^^^^^ ^^

Don't they mean "wasn't"? The rest of the report seems (to me) to be reasonably detailed, well explained, and apparently honest, but this one little dissemblance ruins the whole thing. Is there any justification for the assertion that the prediction was (and is) \_impossible\_ in these circumstances?

-- Bob Munck, MITRE Corporation, McLean VA

---

**✂ Re: Airbus crash of June 88**

*Robert Dorsett <rd@walt.cc.utexas.edu>*

*Thu, 1 Feb 90 02:23:53 CST*

In [RISKS 9.63](#), Olivier Crepin-Leblond provided a number of interesting conclusions regarding the A320 crash at Mulhouse-Habsheim. \_Flight International\_ also leaked the commission's findings, which accord heavily with what he translated. It should be noted, however, that while the engines were at comparatively high power settings at the time of impact, the flight path of the airplane was quite unusual -- it approached the field from a high altitude, "dirty" (flaps and landing gear extended), and with engines at *\*flight idle.\** It is entirely conceivable that the airplane was far behind the power curve at the point the flight crew decided to go around; moreover, this maneuver is unusual enough in of itself to bring into serious doubt the crew's judgement.

The altimeter issue is also interesting, but has largely been applied to the incident after later experiences with altitude displays going haywire on IFR approaches (including one well-publicised incident into Zurich). In the crash, the visibility was unlimited VFR; at low altitudes in such weather, one does not pay much attention to the altimeter, anyway--even in airliners. The captain still insists that his flight instruments did him in.

Lastly, I note with some amusement the captain's new place of employment. Australia has been undergoing a very bitter pilot's dispute. The largest airline recently fired all striking pilots (which is to say, all of its pilots) and has been recruiting heavily overseas, offering relatively senior positions to anyone with even marginal qualifications.





Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 9: Issue 65

Friday 2 February 1990

## Contents

- [The C3 legacy, Part 2: a SAGE beginning](#)  
[Les Earnest](#)
- [Sendmail Flaw](#)  
[Geoffrey H. Cooper](#)
- [Filing 1040 Electronically](#)  
[Bill Murray](#)
- [Predicting Problems](#)  
[David desJardins](#)
- [Airbus crash](#)  
[Dave Morton](#)
- [The Trojan horse named 'AIDS' revisited](#)  
[PGN](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✉ The C3 legacy, Part 2: a SAGE beginning

*Les Earnest* <LES@SAIL.Stanford.EDU>  
01 Feb 90 2101 PST

Thanks to [moraes@csri.toronto.edu](mailto:moraes@csri.toronto.edu) for pinning down my half-remembered quotation in the preceding segment ([RISKS 9.60](#)):  
> The actual quote is "Those who cannot remember the past are condemned  
> to repeat it." from George Santayana's "The Life of Reason".

The grandfather of all command-control-communication (C3) systems was an air defense system called SAGE, a rather tortured acronym for Semi-Automatic Ground Environment. As I reported earlier in [RISKS 8.74](#), some of the missiles that operated under SAGE had a serious social problem: they tended to have inadvertent erections at inappropriate times. A more serious problem was that SAGE, as it was built, would have worked only in peacetime. That seemed to suit the Air Force just fine.

SAGE was designed in the mid to late 1950s, primary by MIT Lincoln Lab, with follow-up development by IBM and by nonprofits System Development

Corp. and Mitre Corp. The latter two were spun off from RAND and MIT, respectively, primarily for this task.

SAGE was clearly a technological marvel for its time, employing digitized radar data, long distance data communications via land lines and ground-air radio links, the largest computer (physically) built before or since, a special-purpose nonstop timesharing system, and a large collection of interactive display terminals. SAGE was necessarily designed top-down because there had been nothing like it before -- it was about 10 years ahead of general purpose timesharing systems and 20 years ahead of personal computers and workstations.

While the designers did an outstanding job of solving a number of technical problems, SAGE would have been relatively useless as a defense system if a manned bomber attack had occurred for the following reasons.

1. COUNTERMEASURES. Each SAGE system was designed to automatically track aircraft within a certain geographic area based on data from several large radars. While the system worked well under peacetime conditions, an actual manned bomber attack would likely have employed active radar jamming, radar decoys, and other countermeasures. The jamming would have effectively eliminated radar range information and would even have made azimuth data imprecise, which meant that the aircraft tracking programs would not have worked. In other words, this was a air defense system that was designed to work only in peacetime!

(Some "Band-aids" were later applied to the countermeasures vulnerability problem, but a much simpler system would have worked better under expected attack conditions.)

2. HARDENING. Whereas MIT had strongly recommended that the SAGE computers and command centers be put in hardened, underground facilities so that they could at least survive near misses, the "bean counters" in the Pentagon decided that this would be too expensive. Instead, they specified above-ground concrete buildings without windows. This was, of course, well suited to peacetime use.

3. PLACEMENT. While the vulnerabilities designed into SAGE by MIT and the Pentagon made it relatively ineffective as a defense system, the Air Defense Command added a finishing blunder by siting most of the SAGE computer facilities in such a way that they would be bonus targets! This was an odd side effect of military politics and sociology, as discussed below.

In the 1950s, General Curtis Lemays's Strategic Air Command consistently had first draw on the financial resources of the Defense Department. This was due to the ongoing national paranoia regarding Soviet aggression and some astute politicking by Lemay and his supporters. One thing that Lemay insisted on for his elite SAC bases was that they have the best Officers Clubs around.

MIT had recommended that the SAGE computer facilities be located remotely, away from both cities and military bases, so that they would not be bonus targets in the event of an attack. When the Air Defense Command was called upon to select SAGE sites, however, they realized that their people

would not enjoy being assigned to the boondocks, so they decided to put the SAGE centers at military bases instead.

Following up on that choice, the Air Defense Command looked for military bases with the best facilities, especially good O-clubs. Sure enough, SAC had the best facilities around, so they put many of the SAGE sites on SAC bases. Given that SAC bases would be prime targets in any manned bomber attack, the SAGE centers thus became bonus targets that would be destroyed without extra effort. Thus the peacetime lifestyle interests of the military were put ahead of their defense responsibilities.

SAGE might be regarded as successful in the sense that no manned bomber attack occurred during its life and that it might have served as a deterrent to those considering an attack. There were reports that the Soviet Union undertook a similar experimental development in the same time period, though that story may have been fabricated by Air Force intelligence units to help justify investment in SAGE. In any case, the Russians didn't deploy such a system, either because they lacked the capability to build a computerized, centralized "air defense" system such as SAGE or had the good sense not to expend their resources on such a vulnerable kludge.

(Next segment: command-control catches on.)

-Les Earnest (Les@Sail.Stanford.edu)

---

## ✂ Sendmail Flaw

*Geoffrey H. Cooper <geof@aurora.com>  
Fri, 2 Feb 90 14:35:37 PST*

The sendmail problem to which our moderator frequently refers is actually a design problem in the SMTP protocol (that sendmail implements) and so is well within the domain of RISKS discussions. Especially since the design problem has been recognized since at least 1983, but SMTP is so entrenched that the problem has never been fixed.

The way in which SMTP sends a message is, roughly:

1. Send message headers to server, etc. & get responses
2. Send DATA keyword to server & get affirmative response
3. Send entire message to server with no response
4. Send "." to Server
5. WAIT UNTIL SERVER HAS DELIVERED MESSAGE AND RESPONDS.

[5] is the problem. At any given time during [5], there are two possibilities. Either the server has crashed and will never send an answer, or the server is still in the process of transmitting the mail.

There is NO WAY for the sender to tell the difference between these two possibilities. This is because:

- a. SMTP presumes that TCP is reliable, so it doesn't allow the sender to retransmit anything. Hence, the sender can't send any data during the wait in [5] to find out if the server is still alive.
- b. TCP, to be efficient for long lived connections, does not guarantee continual monitoring of the connection. If TCP has no data to send, it never sends any data (except for the Berkeley-derived keep-alive option, which are not part of the TCP spec, but see below).
- c. EVEN IF TCP did monitor the connection, the SMTP process could die or go into an infinite loop without resetting the TCP connection. (You can't catch this case: Halting Problem). I can vaguely remember hearing of this happening in 1983.

I truly believe this problem is unsolvable, without changing SMTP. The Programming Marines, who build and sell systems must solve it anyway. Or alleviate it, anyway.

The ad-hoc solution is to set a timeout; assume the message takes no more than time T to process by the server, so if the sender waits for 2T or so, the server must have crashed. This helps, but it clearly doesn't solve the problem, since the sender has no metric by which to judge T except the length of the message.

For example, a message transmitted to a Large, Risky Mailing List might take an order of magnitude longer to process than a simple user-to-user message. Hence, it is likely that messages to large mailing lists will tend to fail with the sender timing out and resetting the connection; this condition is noticed by the server AFTER transmitting at least part of the message. The sender later retries, so you get multiple messages. Very many messages, if you are unlucky, or its a Monday or you moderate a very large and risky mailing list.

(BTW, it was decided in SMTP's design that it was better to have multiple messages than to have messages get lost, so it is not considered acceptable for the SMTP server to queue the message but not deliver it during the pause in [5]).

The general problem: building functionality on top of a "reliable system" does not GUARANTEE that the result is reliable. The reliability must, in some way, be verified by the topmost level.

Hence, you balance your bank statement to make sure your checks (cheques.uk) were really cashed shortly after you sent them off, and you look for cancel checks if you get a red notice from a bill you sent off.

Reference:

J. Saltzer, D. Reed, D. Clark, "End-to-End Arguments in System Design", Proc. IEEE, April 1981.

- Geof

[Well, on [RISKS-9.64](#) I removed all of the offending addresses and I did not get any reports of multiples. So, here goes [RISKS-9.65](#). PGN]

---

### **✦ Filing 1040 Electronically**

<WHMurray.Catwalk@DOCKMASTER.NCSC.MIL>

*Fri, 2 Feb 90 17:47 EST*

It is now possible for you to file your income tax return electronically. Yes, you. Of course the IRS will not accept it directly from you; they only deal with "tax preparers" like H&R Block, the owners of CompuServe. Not to worry. There are value-added re-sellers who will accept your return from you, check it and forward it to the IRS. I have seen ads now from two different such re-sellers: "Nelco" and "Nexus Direct."

PGN's misgivings to the contrary notwithstanding, it is not likely to open up the IRS's computers to tampering by taxpayers. From their point of view it is as safe as having you send it to them by snailmail and a lot cheaper than key-entering it themselves.

From the taxpayers' point of view, it is a great deal safer than putting it in the snailmail and having it transcribed by a temp at the IRS. Of course, a copy of your return can end up in the computers of the services. On the other hand, that happens whenever you deal with a tax preparer. That has only marginally impacted the success of H&RB.

Incidentally, when you file with H&RB, or any number of other preparers, they offer to give you your refund on the spot. It is really in the form of a loan, but the loan is re-paid directly to them by the IRS. The IRS likes this arrangement because they can pay the refund by EFT/EDI. Not only do they not handle the paper return, but they do not have to prepare a check for the refund. It is almost as if the IRS has opened thousands of offices across the country where they will prepare your return for you and give you your refund on the spot. Of course, since it is for-profit, it may be a little more efficient.

Who pays? Well who always pays? At least there are some choices.

How about it H&RB? How long will it be before I can "GO 1040" on CompuServe?

William Hugh Murray, Fellow, Information System Security, Ernst & Young  
2000 National City Center Cleveland, Ohio 44114  
21 Locust Avenue, Suite 2D, New Canaan, Connecticut 06840

---

### **✦ Predicting Problems**

David desJardins <desj%idacrd@Princeton.EDU>

*Fri, 2 Feb 90 01:05:48 EST*

Bob Munck <munck@community-chest.mitre.org> writes:

<> While the software had been rigorously tested in laboratory  
<> environments before it was introduced, the unique combination of  
<> events that led to this problem couldn't be predicted.

>

> Don't they mean "wasn't"? The rest of the report seems (to me) to  
> be reasonably detailed, well explained, and apparently honest, but  
> this one little dissemblance ruins the whole thing. Is there any  
> justification for the assertion that the prediction was (and is)  
> impossible in these circumstances?

I noticed this too. On reflection, though, I'm sort of glad that they said it this way. Of course this error could have been predicted. Any particular error could be predicted, if the right person looked at it at the right time. But what *is* impossible is to predict all errors, all of the time, with probability 1. So, if you interpret the above statement above as, "The event occurred randomly in a situation where the probability of such errors could not be reduced to zero," then I think it is a reasonable description of the truth.

Certainly it is a better reaction than the other common thing that one sees in these press statements, which is something like, "Steps are being taken to ensure that no similar outage can ever occur again." This is an unrealistic and false reaction which would cause me, at least, far more concern than the AT&T reaction. Of course they will try to prevent such problems. But it is equally obvious that the probability of such events will remain positive.

-- David desJardins

---

## ✂ Airbus crash

*Dave Morton <dave@ecrcvax.UUCP>*

*Fri, 2 Feb 90 09:22:30 +0100*

Coming back from London about a year ago I was seated next to a pilot from a Munich based company who flew 757s. He'd overshot his flying time and was heading back to Munich from Kenya over London. We talked about the Airbus crash and it seems that in pilot circles it was attributed to the fact that the older Airbus machines had Rolls-Royce engines. It seems that when given full power they reacted about 3 seconds faster than those on the A320. In his opinion these three seconds were vital. Needless to say, the A320 pilot was familiar with the older model(s) and this may have played a role in his judgement. On a side note the pilot also mentioned that the 757, which also has the fly by wire system, sometimes "hangs". The only way to get the electronics to function again is to power cycle the lot.

---

## ✂ The Trojan horse named 'AIDS' revisited ([RISKS-9.55](#))

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

*Fri, 2 Feb 90 15:58:21 EST*

We reported earlier on the diskettes containing a destructive Trojan horse program. Something like 20,000 disks were mailed from London around 11

December 1989. When executed, it trashed PCs in at least Britain, Norway, Sweden, Belgium, Denmark and California.

Joseph W. Popp, 39, a zoologist from the Cleveland area, has been arrested in Ohio on a federal fugitive warrant, and charged by Scotland Yard in London with blackmail and extortion. In court in Cleveland, Popp told U.S. Magistrate Joseph W. Bartunek he is under a psychiatrist's care and must take drugs for a mental condition. The judge has scheduled psychiatric evaluation prior to any further hearing. Popp apparently (has/had?) worked for the World Health Organization.



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

**Volume 9: Issue 66**

**Monday 5 February 1990**

## Contents

- [Another SAGE memoir](#)  
[Jon Jacky](#)
- [DoD plans another attack on the "software crisis"](#)  
[Jon Jacky](#)
- [The Cultural Dimensions of Educational Computing](#)  
[Phil Agre](#)
- [Vincennes' Aegis System: Why did RISKS ignore specifications?](#)  
[R. Horn](#)
- [Computer Virus Book of Records](#)  
[Simson L. Garfinkel](#)
- [Re: AT&T](#)  
[Gene Spafford](#)  
[David Keppel](#)  
[Stanley Chow](#)
- [Sendmail](#)  
[Brian Kantor](#)  
[Rayan Zachariassen](#)  
[Geoffrey H. Cooper](#)  
[Kyle Jones](#)  
[Craig Everhart](#)
- [Re: Risks of Voicemail systems](#)  
[Randall Davis](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **✉ Another SAGE memoir**

*Jon Jacky <JON@GAFFER.RAD.WASHINGTON.EDU>*  
*Sun, 4 Feb 1990 14:46:36 PST*

Les Earnest's posting on SAGE reminded me of an anecdote James Fallows tells in his book, NATIONAL DEFENSE (Vintage Books, 1982, p. 59):

"As a child in California, I grew up five miles from SAGE headquarters at Norton Air Force Base. Each year our classes would take school field trips

to Norton. The dramatic conclusion came when we were ushered into the SAGE control room. The commanding general would appear at this point and attempt a demonstration of how quickly and reliably his system worked. In every instance I can remember, there was a technical screw-up of some kind, and the general would lead us out, assuring us that, heh heh, this sort of thing did not happen very often."

Much of Fallows' book is a critique of technically complex weapons systems, which many readers of this digest would find interesting. Fallows summarizes the SAGE story this way (also on p. 59):

"Wouldn't it be wonderful if, instead of leaving aerial combat to a group of pilots trying to figure it out for themselves which enemy planes to destroy, the whole enterprise could be automatically controlled from the ground? If you had a huge radar and computer complex, it might be able to identify all the "friendly" and "enemy" planes in the sky and rationally distribute assignments for shooting them. Then it could transmit commands to each fighter plane, guiding it precisely to its target. Visions of this sort lay behind a \$20 billion radar complex of the sixties known as SAGE --- which, after countless revisions, finally foundered due to the technical complexity of devising a computer program that could keep the friendly and enemy planes straight. Nonetheless, the Air Force and Navy have invested further billions in radar planes known as the AWACS and E-2, which face the far greater technical challenge of doing the same thing from a single plane in the air."

In a footnote Fallows says more of the technical difficulties of distinguishing friend from foe:

"The real problem was that since planes in a dogfight fly in unpredictable patterns, when two "blips" from two planes crossed on the radar screens the computer could not be sure which plane was which when they separated again. ..."

(Fallows doesn't give a source for this explanation of the foundering of SAGE; the more usual explanation is that SAGE became obsolete after the Soviet Union concentrated on aiming ICBM's, rather than manned bombers, at the continental U.S.A. I remember a local news story around 1982 saying they were finally shutting down the SAGE installation at McChord Air Force Base near Seattle, Washington).

- Jon Jacky, University of Washington

---

### **🚨 DoD plans another attack on the "software crisis"**

*Jon Jacky <JON@GAFFER.RAD.WASHINGTON.EDU>  
Sun, 4 Feb 1990 15:23:21 PST*

Here are excerpts from ELECTRONICS ENGINEERING TIMES, Jan 29 1990, p. 16:

DOD PLAN ADDRESSES SOFTWARE PROBLEMS by Brian Robinson

Washington - The Defense Department is expected to go public next month with an

ambitious plan aimed at solving its growing software problems. The product of an agency-wide collaboration, the plan represents the first time the Pentagon has managed to get a broad consensus on the issue.

The master plan, to be implemented over five years, will tackle the rapidly expanding size and development costs of defense software, a problem made worse by the tendency of different groups within the Pentagon to go their separate ways when it comes to software requirements.

Some 20 groups within the defense community reportedly took part, including the Army, Navy, Air Force, Defense Communications Agency, National Security Agency, and the Defense Advanced Research Projects Agency.

The plan covers six major topics: software acquisition and life cycle management, government software policies, organizational coordination and cooperation, personnel, the software technology base and software technology transition. ...

Pentagon analysts have predicted growing problems as military systems expand in size and complexity and as projects are developed that require programs with many millions of lines of code, the Strategic Defense Initiative being the prime example. ...

A House investigations subcommittee report late last year accused the Defense Department and other federal agencies of putting lives at risk and wasting billions of dollars with substandard software ...

The National Research Council also condemned the current state of software and development practices, contending that researchers in government and industry had not kept up with the development of complex software systems.

The DoD will collect public comments on the plan at a forum April 3 -- 5 in Falls Church, VA.

(The article does not mention who, or which agency, was the source of this story. The article also does not mention any of the DoD agencies and projects already charged with this problem, including STARS, SEI, AJPO, or the 1987 Defense Science Board study).

- Jon Jacky, University of Washington

---

## **✶ The Cultural Dimensions of Educational Computing**

*"Phil Agre" <agre@gargoyle.uchicago.edu>*

*Sun, 4 Feb 90 18:05:30 199*

Anyone who is interested in technology as a cultural phenomenon will probably want to read the following book:

C. A. Bowers, *The Cultural Dimensions of Educational Computing: Understanding the Non-Neutrality of Technology*, Teacher's College Press, 1988.

It is often said that computers are neutral in that, like pencils and hammers, they can be used for either good or evil. This might be true on some possible interpretations, but Bowers argues that it is false on a long list of others. Specifically, he argues that particular computer systems for education often incorporate unarticulated assumptions about computers, about thinking, about society, and about the relations among these things, and that the use of these systems can inculcate or reinforce the uncritical, even unwitting acceptance of those assumptions by students and teachers alike. He gives many examples, and his arguments seem to me to apply equally well to a wide variety of other applications of computers. In developing his arguments, he touches on a wide variety of critiques of technology and of computation as social phenomena. Although he has done a valuable public service in presenting these ideas in accessible ways, the principal weak spot of the book is a sometimes excessive credulity toward the critiques themselves, which are not of uniform quality. Reading him thus calls for a critical and selective attitude as well as an open mind, but then it is exactly his point that we should bring such an attitude to everything that concerns technology. Highly recommended.

---

### **✦ Vincennes' Aegis System: Why did RISKS ignore specifications?**

*<HORN%HYDRA@sdi.polaroid.com>*

*Mon, 5 Feb 90 09:15 EST*

Recent continuation of the Vincennes controversy in the Naval press spurs an observation:

When faced with a catastrophic failure, the non-computer naval community is analyzing the system specifications and comparing them with the actions taken (albeit non-mathematically). When faced with the same catastrophe, the RISKS community utterly ignored the specifications and lept into discussion of potential software flaws and changes. This from a group where proof of conformance to specification has a strong following.

By specifications I refer not to the engineering documents used in building the shipboard equipment. I mean the laws and treaties governing the behaviour of combatant and non-combatant in areas of conflict. They did and do have direct relevance to the computer systems.

There have been at least five relevant treaties covering such behaviour in the last century. There is a tremendous literature exploring issues and alternatives. Situations like the Vincennes are explicitly explored and analyzed. These are the recognized specifications for how all parties should behave.

I am not interested in renewing controversy over the events. Parties interested in the relevant treaties and laws might start with the overview in International Law for Seagoing Officers, Roberts, and branch out from there into details and current discussions.

I am interested in some introspective analysis of why the computer community of RISKS totally ignored the specifications. Understanding this behaviour can

lead to understanding a common failure mode of computer systems.

Was it ignorance? If so, why no requests for information? Why such willingness to proceed in ignorance?

Was it fear that the discussion of treaty and law might degenerate into political arguments? If so, how can systems involving political sensitivity be subject to specification and analysis?

Was it other group dynamics? If so, how can these be controlled productively? (In my own case I would place this as dominant. I became interested in the discussions and overlooked the growing irrelevancy. Furthermore, the group dynamic discouraging radical departures from the current topic of discussion made me hesitate to change topics.)

What other factors were involved?

I can think of only one invalid excuse. Unlike most systems, these specifications are readily available to the public world wide.

R Horn horn%hydra@polaroid.com

[I don't think the RISKS community completely ignored the `specifications'. See my summary of Matt Jaffe's discussion, [RISKS-8.74](#), 26 May 1989. PGN]

---

## **Computer Virus Book of Records**

*Simson L. Garfinkel <simsong@prose.CAMBRIDGE.MA.US>  
4 Feb 90 14:46:06 EST (Sun)*

(This is chart 74 from the National Center for Computer Crime Data's 1989 report, Commitment to security.) Please forgive any typos.

\$97,000,000 John McAfee's estimate of the cost of the "Internet Worm."  
[John McAfee is president of the Computer Virus Industry Association.]

\$10,000,000 Cliff Stoll's estimate of cost of "Internet Worm."  
(See \$100,000.)

250,000 Richard Brandow's estimate of the number of computers his "World Peace Virus" infected.

\$250,000 Cost of reacting to "Internet Worm" at Los Alamos National Laboratory.

\$200,000 Gene Spafford's estimate of cost of "Internet Worm."

168,000 Records destroyed by one computer trojan horse planted in Texas.

\$100,000 Cliff Stoll's low bound estimate of cost of "Internet

- Worm" (see \$97,000,000)
- \$72,500 NASA Ames' estimate of its loss from "Internet Worm"
- 8,000 Gene Spafford's estimate of personnel hours lost battling "Internet Worm"
- 6,000 NCCD's estimate of number of these hours which were not compensated.
- 6,000 Most common estimate of the number of computers affected by "Internet Worm."
- 3,000 Copies of "world peace" virus found in Aldus software
- 2,000 Cliff Stoll's estimate of the number of computers infected by the "Internet Worm."
- 800 Computer virus incidents reported to Computer Virus Industry Association in first 8 months of 1988 (see 96)
- 130 Countries in which computers were infected by "Christmas Tree" virus
- 96 Percentage of reports received by Computer Virus Industry Association which incorrectly identified viruses.
- 53 Percentage of National Center survey respondents who expected to be using anti-virus software in 1991
- 28 Articles about viruses listed in Reader's Guide to Periodical Literature in 1988 (see 1)
- 22 Percentage of National Center security survey respondents who were using anti-virus products in 1988 (see 1.5)
- 21 Editorials arguing that the "Internet Worm" demonstrates the need for greater commitment to security (see 10).
- 14 Computer virus cartoons collected at NCCCD
- 10 States currently considering new computer crime laws to fight viruses
- 10 Letters to the editor saying we should applaud rather than punish those who set loose computer viruses (see 21)
- 8 Letters to the editor and columns calling for punishment of those who set loose computer viruses (see 10)
- 7 Editorials calling for tough law enforcement against computer virus vandals.

- 6 Books in English on viruses
- 5 Years since term "virus" was coined.
- 5 Publicized calls for computer ethics in light of "Internet Worm"
- 4 State computer crime law virus prosecutions
- 2 Civil suits over viruses
- 1.5 Percentage of national Center survey respondents who were using anti-virus products in 1985. (See 22,53)
- 1 Articles about viruses listed in Reader's Guide to Periodical Literature in 1987 (see 28)
- 1 Federal computer crime law virus prosecutions.

---

**Re: AT&T ([RISKS-9.62](#))**

*Gene Spafford <spaf@cs.purdue.edu>  
27 Jan 90 17:52:42 GMT*

In article <CMM.0.88.633398480.risks@hercules.csl.sri.com> risks@csl.sri.com writes:

>From Telephony, Jan 22, 1990 p11:

>

- > The problem began the afternoon of Jan 15 when a piece of trunk
- > interface equipment developed internal problems for reasons that
- > have yet to be determined.

An interesting twist to this: several members of the media have gotten phone calls from a rogue hacker claiming that he and a few friends had broken into the NYC switch and were "looking around" at the time of the incident.

This raises two interesting (at least to me) possibilities:

- 1) They had, indeed, broken in, and were responsible for the crash. (Don't blindly accept published statements from AT&T that it was all a simple glitch. Stories told off-the-record by law enforcement personnel and telco security indicate this kind of break-in is common.)

If this is true, what to do from here? Obviously, this raises some major security questions about how best to protect our phone systems. It also raises some interesting social/legal questions. The nationwide losses here are probably greater than the Internet Worm, but the Federal Computer Crime and abuse act don't cover it (only one system tampered with). Other laws maybe cover it, but is there any hope of proving it and prosecuting?

2) These guys were not on the machine but are trying to get the press to publish their names as the ones responsible. This would greatly enhance their image in the cracker/phreaker community. It's akin to having the Islamic Jihad call up and claim that a suicide caller had crashed the system (to protest dial-a-prayer and dial-a-porn, perhaps; remember that the Great Satan is a local call from NYC :-). It raises interesting questions about how the press should handle such claims, and how we should react to them.

A third possibility exists, of course, that those guys had hacked into the switch, but they had nothing to do with the failure. That raises both sets of questions.

I worry that it won't be long before this kind of thing happens and the phone calls ARE from some terrorist group claiming responsibility: "We are holding your dial tone hostage until you get your troops out of Panama, make abortion illegal, stop killing animals for fur, and prevent Peter Neumann from making more puns."

Or, perhaps AT&T security gets a call like: "We've planted a logic bomb in the switching code. Put \$1 million in small unmarked bills in the following locker at the bus station, or in 4 hours every call made in Boston will get routed to dial-a-porn numbers in NYC. We'll tell you how to fix it as soon as we get the money."

Any bets that something like this will happen this year? Last year's WANK worm and politically-motivated viruses seem to suggest the time is ripe.

Gene Spafford, NSF/Purdue/U of Florida Software Engineering Research Center,  
Dept. of Computer Sciences, Purdue University, W. Lafayette IN 47907-2004  
uucp ...!{decwrl,gatech,ucbvax}!purdue!spaf

[By the way, AT&T is certain it was an open&shut (a no-pun&shut?) case of a hardware-triggered software flaw, reproducible in the testbed ... PGN]

---

**✉ Re: AT&T ([RISKS-9.63](#))**

David Keppel <pardo@cs.washington.edu>  
1 Feb 90 02:26:40 GMT

In RISKS 9:63, Willaim Murray (WHMurray.Catwalk@DOCKMASTER.NCSC.MIL) writes:  
>AUTOMATE ONLY THOSE THINGS THAT HAPPEN WITH SUFFICIENT FREQUENCY THAT  
>AUTOMATION IS JUSTIFIED. AVOID GRATUITOUS AUTOMATION.

``Sufficient frequency" should be qualified. When I was a system manager I was frequently glad that our Unix would reboot itself after minor panics.

That reminds me of a chap named Ferguson who built cars in the 60's. They had 4-wheel drive and anti-skid braking. He said ``They [the safety features] only need to save your life \*once\* to have them pay for themselves."

; -D on ( Rhino boot ) Pardo

---

**✉ Re: AT&T ([RISKS-9.62](#))**

Stanley Chow <[schow@bcarh185.BNR.CA](mailto:schow@bcarh185.BNR.CA)>

Wed, 31 Jan 90 00:30:14 EST

I would like to make a comment regarding the AT&T incident.

I want to state clearly that I work for Bell-Northern Research. We are the R&D arm of Northern Telecom, which happens to be in hot competition with AT&T. In particular, I work on the DMS switches, for which 4ESS is the prime competition. In no way do I represent the official views of BNR or NT. What follows is strictly the observations of a computer professional.

The article does not answer the key question:

How can such a simple and REPRODUCIBLE bug be released to the field? Especially in such a critical arena?

Note that a number of things had to happen:

- 1) The failure of a single piece of equipment turns into the (perceived) failure of all equipment at the same site. Thus, "Multiplying" the problem.

I.e., recovery of a single trunk ends up sending messages out through ALL trunks.

- 2) Recovery action of "healthy" sites ends up "Spreading" the problem.

The recovery of a truck should not cause the collapse of the whole site.

- 3) Testing does not catch the problem.

The problem is reproducible and should have been caught in a pre-release simulated real-life testing of the error recovery system.

All of these are likely flaws are in any system. Error recovery is rarely needed - on most systems, you just reboot the machine or just logoff/logon to your account again. As a result, most people don't think about error recovery much less test it. Unfortunately, error recovery is very difficult to design and even harder to test.

Stanley Chow, BNR BitNet: [schow@BNR.CA](mailto:schow@BNR.CA) UUCP: [..!psuvax1!BNR.CA.bitnet!schow\(613\)763-2831..!utgpu!bnr-vpa!bnr-rsc!schow%bcarh185](mailto:..!psuvax1!BNR.CA.bitnet!schow(613)763-2831..!utgpu!bnr-vpa!bnr-rsc!schow%bcarh185)

---

**✉ Re: sendmail flaw**

Brian Kantor <[brian@ucsd.edu](mailto:brian@ucsd.edu)>

Fri, 2 Feb 90 22:12:52 -0800

It is not an SMTP requirement to complete delivery between receipt of the "." signifying the end of the message and returning the "250 OK" message. It is perfectly valid to simply store the message and return the OK; you do NOT have to deliver in real time while the sender waits.

That sendmail often does this is perhaps a common flaw, but don't confuse it with any RFC requirement! It's valid to accept the message and mail back a delivery failure later. Probably sendmail should do that.

The most common cause of long waits is expanding mailing lists; sometimes this takes so long that the sender times out and resends the message on the assumption that it's failed. However, the recipient sendmail believes it to have succeeded, so lots of people gets lots of copies of the message until such time as the network environment lets things happen within the timeout limits.

We at UCSD have most of our mailing lists explode in deferred time so that an incoming message for one of them is just stored and immediately acknowledged. It is then delivered later.

Another common reason for long waits between "." and "250 OK" is the time taken to process headers; if that invokes calls to the system nameserver to look something up in the DNS, there might well be a delay. That's not good planning but lots of people do it.

Sending sites probably ought to have their timeout set to around 15 minutes to a couple of hours to avoid these problems, at least until sendmail is fixed.

Finally, sendmail has a tendency to do invalid longjumps on timeouts of various kinds: occasionally the stack is bugged and the longjump winds up causing it to die horribly, leaving the list of delivered addresses un-updated. Then the next queue run happens and the people early on the list get the message again and again and again....

I've heard rumors of a patch to sendmail that makes it checkpoint the delivery list (the qf file) after every successful delivery. That solves that problem, but it's really a bandaid on the bad longjump problem. I don't have a copy of that patch.

I know people swear at sendmail; it's a difficult program to understand and it's been worked on by a lot of people, so some degree of bit-rot has indeed set in. But I'm pleased that it works as well as it does. It just happens to be one of those programs that causes maximum user annoyance when it goes wrong.

brian@ucsd.edu ucsd!brian

Brian Kantor, UCSD Network Operations, UCSD C-024, La Jolla, CA 92093-0124

---

**✉ Re: Sendmail Flaw**

*Rayan Zachariassen <rayan@cs.toronto.edu>  
Sat, 3 Feb 90 16:37:14 EST*

I would rephrase the SMTP problem slightly, and draw different conclusions:

After the message terminator (". " CRLF) has been sent, there are three possible states:

1. The server SMTP crashes before accepting responsibility for delivery (defined by receipt of an OK code at the client SMTP).
2. The server SMTP crashes after accepting responsibility for delivery but before it can deliver the OK code to the client SMTP.
3. The server SMTP doesn't crash.

What makes this bad is that during synchronous delivery, the final acceptance OK code isn't returned until the server SMTP has delivered the message to its recipients. If the recipient is really an address exploder, some addresses may be processed to completion before the server SMTP crashes. This is a state 1 condition because the server SMTP has implicitly accepted responsibility for delivery to *\*some\** of the recipients of the message, but not yet all.

There is also a vulnerable window in state 2 above. You would think that the window is very small, but there is ample opportunity for a swapout or some other act-of-God delay in the execution of the acknowledgement delivery, during which time the server can crash.

Both of these seem to happen more frequently than people thought.

# (BTW, it was decided in SMTP's design that it was better to have multiple # messages than to have messages get lost, so it is not considered acceptable # for the SMTP server to queue the message but not deliver it [synchronously]).

On the contrary, the server SMTP may do anything it wants as long as it takes responsibility for delivery of the message. In particular this means using asynchronous delivery, after simply queueing the message to decrease the vulnerable window (of state 1). Some people like the 'real-time' feedback of synchronous delivery, but it is a dangerous thing to like given the cost.

There are economic arguments for doing synchronous address verification in the SMTP protocol (if you are on a volume-charged network, you don't want to transfer the message data until you know the server SMTP knows what to do with the message), but doing so also leads to instability on client SMTP computers as queues build up waiting for a slow server.

Barring economic/bandwidth issues, in message transfer the HOT ROCK model is very appropriate: you try to get rid of a queued message as quickly as possible, by almost any means. This requires asynchronous checking and delivery in server SMTPs.

See also RFC1047 by Craig Partridge on "Duplicate messages and SMTP".

rayan

**✉ Re: Re: sendmail flaw**

Geoffrey H. Cooper <geof@aurora.com>

Sat, 3 Feb 90 18:43:03 PST

Thanks for your message.

- > It is not an SMTP requirement to complete delivery between receipt of
- > the "." signifying the end of the message and returning the "250 OK"
- > message.

I stand corrected. The problem I bring up is in the design of the protocol and the consequent generalization to software design. It would be different if the protocol spec SPECIFIED that no processing was to be done during this time. That would certainly diminish the problem, and one could make the valid argument that this fixes the problem "enough." After all, by the same top-level reliability argument, SMTP itself can never guarantee truly reliable mail (only the sender and recipient of the mail can do that).

- > Another common reason for long waits between "." and "250 OK" is the
- > time taken to process headers; if that invokes calls to the system
- > NAMESERVER to look something up in the DNS, there might well be a
- > delay. That's not good planning but lots of people do it.

(my emphasis added) That one is interesting, since SMTP (and, I admit, my significant exposure to it) somewhat predates domain naming. An example where a lingering bug in a design is made worse by changing system requirements.

- > I know people swear at sendmail.

I'm not one of them. Although I hate debugging sendmail scripts as much as the next system type, I'd much rather do that than deal with binary distribution software that is non-configurable. After all, my systems requirements change from time to time, too.

- Geof

---

**✉ re: Sendmail Flaw**

Kyle Jones <kyle@cs.odu.edu>

Sat, 3 Feb 90 21:09:53 EST

In [RISKS 9.65](#), Geoffrey H. Cooper writes:

- > The sendmail problem to which our moderator frequently refers is
- > actually a design problem in the SMTP protocol [...]
- >
- > (BTW, it was decided in SMTP's design that it was better to have
- > multiple messages than to have messages get lost, so it is not
- > considered acceptable for the SMTP server to queue the message but
- > not deliver it during the pause in [5]).

I never knew of such a design decision. It's certainly not applicable to the mail on the Internet today, considering that the domain system allows mail to be sent to hosts on networks not directly connected to the Internet. Queueing is inevitable since there is no way for the SMTP-server to wait for final delivery on a network that does not support notification of that event.

RFC 821, page 2:

When the recipients have been negotiated the SMTP-sender sends the mail data, terminating with a special sequence. If the SMTP-receiver successfully processes the mail data it responds with an OK reply.

Note the word used is "processes", not "delivers".

The RFC also specifies that if the server finds that it can deliver to some of the recipients but not others, then it should respond with an OK reply, but also compose and send an "undeliverable mail" notification message back to the original sender of the message.

If I were writing an SMTP-server I would take the above as an invitation to queue the message after doing a cursory check of the recipient addresses, send an OK reply, and dispose of the message at leisure, sending error notifications as necessary.

kyle jones <kyle@cs.odu.edu> ...!uunet!talos!kjones

---

## ✉ Re: Sendmail Flaw

<Craig\_Everhart@transarc.com>  
Mon, 5 Feb 90 10:11:48 -0500 (EST)

Certainly Geof Cooper's problem is inherent in SMTP, but I assumed that PGN's distribution problems were more sendmail-specific. To wit: sendmail maintains each outgoing mail message as a pair of files, a qfXXX file listing headers and recipients and a dfXXX file listing the mail body (where the two values of XXX match). Sendmail processes an outgoing mail request by locking the qf/df pair (well, the XXX value) and attempting delivery to each of the recipients listed in the qfXXX file. When it's made an attempt on each recipient, it writes a new qfXXX file recording the recipients to which the mail has yet to be delivered.

In our environment, sendmail executions got interrupted all the time: we rebooted our mail-handling servers daily, and our sendmail processes would get stuck on an SMTP connection for all kinds of reasons. Thus, when our sendmail would start processing a message with many recipients, its run would often be interrupted before it had made a complete pass through all the recipients; in such cases, it would never record the fact that delivery was successful to any of the recipients. The next time sendmail started processing that long list of recipients, it would try 'em all again: bingo, duplicates.

My solution was to have sendmail update the qfXXX file (containing the list of recipients) after every successful delivery. This required a little source-code hacking, but it was very helpful for us. Not only did we stop generating lots of duplicate mail, but we also reduced our mail-processing load so that processing of those many-recipient lists would terminate!

Craig Everhart

---

✉ **Re: Risks of Voicemail systems ([RISKS-9.61](#))**

Randall Davis <davis@ai.mit.edu>

Wed, 24 Jan 90 20:11:14 est

Date: Thu, 18 Jan 90 08:24:18 EST

From: r.aminzade@lynx.northeastern.edu

Subject: Risks of Voicemail systems that expect a human at the other end

Last night my car had a dead battery (I left the lights on -- something that a very simple piece of digital circuitry could have prevented...

Yes, indeed. And the first time that piece of circuitry failed in any interesting, amusing, or dangerous way, 40 people would send articles to RISKS deploring the inexorable trend toward technological overkill in today's society, suggesting how dumb the engineers were to have replaced the good, old fashioned manual switches, and pointing out how that sort of failure NEVER happened with manual switches.

They would of course be right (manual switches fail differently) and they would have forgotten all the dead batteries that didn't happen.

Three morals:

Accidents that don't happen rarely make it into the papers, the public consciousness, or get factored into the ire over failures.

As Don Norman put it rather nicely a while back, the baseline on any technology isn't zero defects. Nothing is perfect now, and for any change the relevant question is how it works, how it fails, and whether on balance it's better than what we had; not whether it's perfect.

There is no free lunch: if you want the convenience, you have to accept the attendant, inevitable risks.

Applying this to the phone system failure, the only perfectly reliable communication medium is none at all; you have to be in the same room with someone. If you want to be someplace else and talk to them, you have to accept the risk of malfunction. And you want direct dial international calls, call waiting, one-touch memory dialing, conference calls, and call forwarding, too? Then accept the risks inherent in increased complexity that inevitably come along. It won't be perfect, but you might be better off than you were.

---



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

**Volume 9: Issue 67**

**Thursday 8 February 1990**

## Contents

- [Shoplifting and Computers](#)  
[Curtis P. Yeske](#)
- [New movie Script writer](#)  
[Olivier Crepin-Leblond](#)
- [Re: Computers, good and evil](#)  
[George L. Sicherman](#)
- [The C3 legacy, Part 3: Command-control catches on](#)  
[Les Earnest](#)
- [Vincennes' ROEs revisited](#)  
[Clifford Johnson](#)
- [SOGS - Hubble Space Telescope software now ready](#)  
[Rodney Hoffman](#)
- [AT&T and reentrant code](#)  
[John A. Pershing Jr](#)
- [AT&T and error recovery](#)  
[Jonathan I. Kamens](#)
- [Dillard's Dept Stores Use SSN as Sales ID - Printed on Receipts](#)  
[Allen Gwinn](#)
- [AutoAlarms](#)  
[Robert J. Woodhead](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **Shoplifting and Computers**

"Curtis P. Yeske" <cy13+@andrew.cmu.edu>  
Mon, 5 Feb 90 17:01:18 -0500 (EST)

>From AP:

...And, experts say, cameras programmed to watch for known shoplifters may someday be used. "It would be programmed to recognize face patterns and analyze the customers as they walk in," said Bob McCrie, editor of New York-based publication Security Letter.

---

## ✂ New movie Script writer

Olivier Crepin-Leblond <zdee699@elm.cc.kcl.ac.uk>

Wed, 7 FEB 90 09:55:52 GMT

Taken from ORACLE Teletext Service (Channel 4, UK):

"Surveying what's available at your local multi-screen, does the feeling ever creep over you that film scripts must be written by a computer ?

You may be right. A recent issue of film mag Hollywood Reporter reveals that a software programme called 'Collaborator' has become available.

It's a 'story structure and script analysis programme', designed to help screenwriters construct their stories.

Somehow the knowledge that it's based on Aristotle's Six Elements of Drama doesn't make me feel any better."

Is big brother now controlling my entertainment ?

Olivier M.J. Crepin-Leblond, Comp. Sys. & Elec. Eng, Electrical & Electronic Eng, King's College London, UK BITNET : <zdee699%elm.cc.kcl.ac.uk@ukacr|>

---

## ✂ Re: Computers, good and evil ([RISKS-9.66](#))

George L Sichertman <gls@odyssey.att.com>

Tue, 6 Feb 90 21:04:22 EST

In \_Risks Digest\_ 9.66 Phil Agre recommends \_The Cultural Dimensions of Educational Computing: Understanding the Non-Neutrality of Technology\_ by C. A. Bowers. Agre's succinct summary begins:

> It is often said that computers are neutral in that, like pencils and  
> hammers, they can be used for either good or evil. This might be true  
> on some possible interpretations, but Bowers argues that it is false on  
> a long list of others. ...

Like many scholars who examine our emerging electronic culture, Bowers is running 25 years behind Marshall McLuhan. Here is McLuhan on the subject of "neutrality":

In accepting an honorary degree from the University of Notre Dame a few years ago, General David Sarnoff [head of RCA -gls] made this statement: "We are too prone to make technological instruments the scapegoats for the sins of those who wield them. The products of modern science are not in themselves good or bad; it is the way they are used that determines their value." That is the voice of the current somnambulism. Suppose we were to say, "Apple pie is in itself neither good nor bad; it is the way it is used that determines its value." ...

There is nothing in the Sarnoff statement that will bear scrutiny, for it ignores the nature of the medium, of any and all media, in the true Narcissus style of one hypnotized by the amputation and extension of his own being in a new technical form. ... It has never occurred to General Sarnoff that any technology could do anything but \_add\_ itself on to what we already are.

\_Understanding Media: The Extensions of Man\_ (1964)

To be fair to Bowers, he may be aware of McLuhan's work. I have not yet read Bowers's book so I cannot say. I \_can\_ say that most of the writers I have read who expound on the unforeseen implications of the electronic age are thoroughly insensible to the unseen implications of the age of print. The risk is that we may regard a necessary consequence of electronic culture as a "risk" to be prevented by suitable countermeasures, because it offends the sensibilities we acquired from print culture.

Col. G. L. Sicherman

---

### **✂ The C3 legacy, Part 3: Command-control catches on**

*Les Earnest <LES@SAIL.Stanford.EDU>*

*05 Feb 90 1523 PST*

(Continuing from [RISKS 9.65](#))

As the U.S. Air Force committed itself to the development of the SAGE air defense system in the late 1950s, new weapons that did not require centralized guidance came to be rejected, even though some appeared to be less vulnerable to countermeasures than those that depended on SAGE. An example was a very fast, long range interceptor called the F-109 that was to carry a radar that would enable it to locate bombers at a considerable distance and attack them. As such, it did not need an elaborate ground-based computer control system.

My group at MIT Lincoln Lab had been responsible for integrating earlier interceptors and missiles into SAGE. We subsequently joined Mitre Corporation when it was formed from Lincoln Lab's rib and were later assigned the responsibility for examining how the F-109 interceptor might be used.

I had assumed that the Air Force was genuinely interested in seeing how the F-109 could best function in air defense. Accordingly, we worked out a plan in which the interceptors that were in service would be deployed to various airfields, both civilian and military, so as to make them less vulnerable to attack. This dispersal together with their ability to function with minimal information about the locations of attacking bombers appeared to offer a rather resilient air defense capability that could survive even the destruction of the vulnerable SAGE system.

When we published a utilization plan for the F-109 based on these ideas, The Air Force made it clear that we had reached the "wrong" conclusion -- we were supposed to prove that it was a bad idea. We apparently had been chosen to "study" it because, as designers of SAGE, we were expected to oppose any

defensive weapons that would not need SAGE.

In order to deal with the embarrassing outcome of this study, a Colonel was commissioned to write a refutation that confirmed the ongoing need for centralized computer control. The Air Force insisted that anyone who requested our report must also get a copy of the refutation. Mitre necessarily acceded. In any case, the F-109 was never built in quantity.

#### The seductive image

Though the designers of SAGE came to recognize its weaknesses and vulnerabilities and the Air Force should have been reluctant to build more systems of the same type, it somehow came to be regarded as the model of what the next generation of military control systems should be. Never mind that it was essentially useless as a defense system -- it looked good!

The upper floor of each SAGE command center had a large room with subdued lighting and dozens of large display terminals, each operated by two people. Each terminal had a small storage-tube display for tabular reference data, a large CRT display of geographical and aircraft information (with a flicker period of just over one second!), and a light gun for pointing at particular features. Each terminal also had built-in reading lights, telephone/intercoms, and electric cigar lighters. This dramatic environment with flickering phosphorescent displays clearly looked to the military folks like the right kind of place to run a war. Or just to "hang out."

Downstairs was the mighty AN/FSQ-7 computer, designed by MIT using the latest and greatest technology available and constructed by IBM. It had:

- o A dual-processor nonstop timesharing system. The off-line computer was usually either undergoing preventive maintenance or was following the actions of the online computer so that it would be ready to take over if that machine failed. In this respect it was similar to the commercial nonstop systems developed much later by Tandem and its followers.
- o The computer was composed of rows of glimmering vacuum tubes spread over an area about the size of a football field, with lots of large magnetic drums used both for secondary storage and as communications buffers. (Magnetic disks had not yet been perfected.)
- o It used the recently-invented magnetic core memories in the largest and fastest configuration yet built: 256K bytes with 6 microsecond cycle time. Each of the two main memories was packed into the volume of a shower stall, a remarkable density for that period.
- o A gigantic air conditioning system was required to suck all the heat out of the monstrous computer.

Remarkably, all of this new technology worked rather well. There were some funny discoveries along the way, though. For example, in doing preventive maintenance checks on tubes, a technician found one that was completely dead that had not been detected by the diagnostics. Upon further examination it was discovered that this tube didn't do anything! This minor blunder no doubt arose during one of the many redesigns of the machine.

Both the prototype and operational SAGE centers were frequently visited by military brass, higher level bureaucrats, and members of Congress. They generally seemed to be impressed by the image of powerful, central control that this leading-edge technological marvel had. Of course, General Lemay and his Strategic Air Command could not sit by and let another organization develop advanced computer technology when SAC didn't have any.

In short order the SAC Control System was born. Never mind that there was not much for it to do -- it had to be at least as fancy as SAGE. When the full name was written out, it became Strategic Air Command Control System. The chance juxtaposition of "Command" and "Control" in this name somehow conjured up a deeper meaning in certain military minds.

In short order, Command-Control Systems became a buzz word and a horde of development projects was started based on this "concept." The Air Force Systems Command soon realized that it had discovered a growth industry and reorganized accordingly. The specifications for the new C2 systems generally contained no quantitative measures of performance that were to be met -- the presumption seemed to be that whatever was being done already could be done faster and better by using computers! How wrong they were.

(Next segment: Command-control takes off)

-Les Earnest (Les@Sail.Stanford.edu)

---

### ✦ Vincennes' ROEs revisited (Horn, [RISKS-9.66](#))

"Clifford Johnson" <GA.CJJ@Forsythe.Stanford.EDU>  
Mon, 5 Feb 90 17:12:48 PST

> By specifications I refer not to the engineering documents used  
> in building the shipboard equipment. I mean the laws and  
> treaties governing the behaviour of combatant and non-combatant  
> in areas of conflict. They did and do have direct relevance to  
> the computer systems.

I for one specifically complained that the U.S. Rules Of Engagement, as implemented and acted upon in the Vincennes incident, were in violation of international law. In this context, the comment of retiring ex-Chairman of the Joint Chiefs of Staff \*Admiral\* Crowe stated in an interview that the biggest change in the military in his lifetime was the change in ROEs, whereby U.S. ships now fired first instead of waiting for a confirmed attack. He stated that missile technology meant you couldn't risk being hit first any more.

---

### ✦ SOGS - Hubble Space Telescope software now ready

Rodney Hoffman <Hoffman.ElSegundo@Xerox.com>  
7 Feb 90 09:50:33 PST (Wednesday)

In [RISKS 8.46](#), Paul Eggert summarized M. Mitchell Waldrop's article "Will

the Hubble Space Telescope Compute?" which appeared in 'Science' magazine 17 March 1989, pp 1437-1439.

The story said "critical operations software is still a mess -- the victim of primitive programming methods and chaotic project management." Supposedly completed in 1986, bugs were still turning up as fast as the programmers could fix them, and the system, the \$70 million Science Operations Ground System (SOGS), ran at only one-third optimum speed. According to the article, the Space Telescope Science Institute, the program managers, were counting on faster computers plus better algorithms plus some (unspecified) AI techniques to fix SOGS. They were confident that SOGS would be ready when the telescope was launched.

Last week, the 'Los Angeles Times' ran a lengthy story about the Space Telescope, but the article did not mention the software. I called the reporter, and he said that he had been at the Space Telescope Science Institute along with other reporters including Waldrop. He says that Waldrop and others did indeed bring up questions about the software, and they were simply told that it's all fine now. We'll soon see. The Hubble Space Telescope is to be launched from the shuttle in an upcoming mission.

---

#### ✂ AT&T ([RISKS-9.62](#)) and reentrant code

*"John A. Pershing Jr." <PERSHNG@IBM.COM>  
Thu, 8 Feb 90 09:55:35 EST*

Reading between the lines of the AT&T pronouncements on the Jan-15 failure, it sounds to me (as a systems programmer) that the "bug" was a reentrancy problem. Specifically, the recovery routine was not reentrant. Under the old way of handling recovery, a single "I'm OK" message would indicate that the previously failed switch was back in service; in the new scheme, the recovery of the failed switch was signalled when new call-setup messages started flooding in, causing the recovery routine to be reentered.

This is sheer speculation on my part; can anyone out there who is "in the know" either confirm or deny this speculation?

John Pershing  
IBM Research, Yorktown Heights

---

#### ✂ AT&T ([RISKS-9.66](#)) and error recovery

*Jonathan I. Kamens <jik@pit-manager.MIT.EDU>  
Mon, 5 Feb 90 19:35:52 -0500*

In a paper entitled "Assuring Quality and Reliability of Complex Electronic Systems: Hardware and Software", published in the January 1988 Proceedings of the IEEE, Edwin A. Irland (who has a whole list of past work for Bell Labs and related companies and whose current position (according to the reprint I have) is as the Assistant Vice President of Switching Analysis and Reliability Technology for Bellcore in Red Bank, NJ) writes the following, which I think is

very much apropos:

... The subtlety of these methods implies an important source of unreliability; unreliable error recovery. Thus it is important that system testing pay meticulous attention to fault simulation to uncover weaknesses in the recovery. Data taken on electronic switching systems show that failure to recover from simplex faults is usually a significant source of total outage time....

A "significant source" indeed...

Jonathan Kamens, MIT Project Athena, jik@Athena.MIT.EDU Office: 617-253-8495

---

### **✂ Dillard's Dept Stores Use SSN as Sales ID - Printed on Receipts**

*Allen Gwinn <allen@sulaco.Sigma.COM>*

*Mon Feb 5 20:29:31 1990*

Subject: DILLARD'S VIOLATING CONFIDENTIALITY - PUBLISHING EMPLOYEE SSN'S  
Newsgroups: misc.consumers,misc.headlines,misc.legal,dfw.general  
Summary: Sanctions possible against employees who don't comply  
Keywords: publish, social security numbers, invasion of privacy

On February 4, 1990, Dillard's Department Stores (headquartered in Little Rock, Arkansas) began using employee's personal Social Security numbers for their employee I.D. and sales associate numbers. These Social Security numbers are visible and, for the time-being, NOT "scrambled" enabling any customer to obtain the Social Security number of any sales associate.

Dillard's plan is to begin "scrambling" the numbers anywhere from two weeks to a month according to various sources. After this process, "nobody will be able to identify [the number] as a Social Security number" according to Ed Auffert, Assistant to the General Counsel. Mr. Auffert added that after the scrambling "gen" has been added to the system, all employees will be required to use their Social Security numbers.

According to a memorandum distributed to all employees recently, employees "must" use their "nine-digit sales numbers" in order to "insure credit for sales rung." The memorandum states that the "terminals will accept three-digit sales numbers" in the interim. In store announcements and other management sources at the Dillard's Department Store at Northpark Center in Dallas have indicated that sales data may not be accurate on employees continuing to use their older three-digit sales codes. Since this data is used to evaluate employee performance, this could mean that employees not desiring to divulge their Social Security numbers to the public could eventually be disciplined or discharged. When contacted personally, Northpark store manager Peter Rodriquez confirmed that employees might be "disciplined" for choosing not to use their personal Social Security numbers even in the interim period (prior to computer "scrambling" of the employee's SSN). After being advised of the intent to use this information as part of a Usenet article, he refused to comment any further and referred further contact to W.R. "Bob" Applebee a regional director for Dillard's in Fort Worth Texas.

Mr. Applebee, when contacted by phone, stated emphatically that the "policy (on the use of Social Security numbers until the encryption was complete) had been rescinded." He stated that at present no employees "anywhere in the Dillard's store system" were using their Social Security numbers. Further, Mr. Applebee stated that these numbers were "not visible on any printed cash register receipts." Contrary to Mr. Applebee's claims, a subsequent check of the Dillard's store in Northpark Center produced several receipts with employee Social Security numbers clearly visible as the sales I.D.

As to the "encryption" method to be used, Dillards officials were unable to provide any details. At least one source familiar with this project feels that it would be possible to decrypt these numbers if comparisons could be made against other encrypted Social Security numbers.

For the mean time, Dillards officials maintain that there is "nothing illegal" about what they are doing. They agree that there are going to be employees that disagree with this policy, but seem to convey the feelings that these people are free to seek employment elsewhere.

More details will be relayed to the appropriate groups as they become available.

Any comments on the matter may be emailed to 'dillard@sulaco.sigma.com' or 'sulaco@dillard'. Any comments received are subject to being relayed to Dillard's headquarters in Little Rock ANONYMOUSLY IF SO INDICATED.

Contacts :

W.R. Applebee, Regional Director (817) 831-5428 Ft Worth, TX  
Ed Auffert, Asst to General Counsel (501) 376-5200 Little Rock, AR  
Peter Rodriquez, Northpark Store Mgr. (214) 373-7000 Dallas, TX

Others either unable to be contacted or refusing comment:

William Dillard, II, President (501) 376-5200 Little Rock, AR  
Gene Baker, Advertising (817) 831-5111 Ft Worth, TX

---

## AutoAlarms

*Robert J Woodhead <trebor@biar.UUCP>  
Tue Feb 6 17:30:00 1990*

Fortunately for many of us, after about 40 years of intense debate in the automotive industry on this complex and challenging "lights on" problem, some manufacturers are adding a simple device that alerts you if your lights are on when the ignition is off. These range from a simple analog "BReeee!" in my Chevy Blazer to digital (shudder!) voice synthesis in some upscale foreign yuppiemobiles.

I for one rate this innovation right up there with Post-It Brand Notes, Microwave Popcorn and VCR's in it's subtle yet sweeping effect on the

whole of Western Society.

;^)

Robert J Woodhead, Biar Games, Inc. !uunet!biar!trebor | trebor@biar.UUCP



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 9: Issue 68

Wednesday 14 February 1990

## Contents

- [Re: Caller ID \(NYTimes editorial\)](#)  
[John M. Sullivan](#)
- [How to make answering machines deliver ransom messages](#)  
[Denis Coskun](#)
- [More on the Hubble Space Telescope](#)  
[Hank Strub](#)
- [Human blamed, not the computer! -- jury duty](#)  
[Lee S. Ridgway](#)
- [Accents are more than just decorations](#)  
[Kai-Mikael J{-Aro](#)
- [\[Parse-ly, Rosemary, Time, Light, Control & Other SAGE Remarks\]](#)  
[Martin Minow](#)
- [Blazers](#)  
[Jeff Berkowitz](#)
- [Re: Computers, good and evil](#)  
[Gregg TeHennepe](#)
- [Telephone Switch Security](#)  
[Roland Ouellette](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **✉ Re: Caller ID (NYTimes editorial)**

*John M. Sullivan <sullivan@math.Princeton.EDU>  
Fri, 9 Feb 90 20:27:26 -0500*

An editorial in the New York Times this morning (Feb 9) entitled "Obscenities, Hang-Ups and Technology" discussed Caller ID, the new phone feature showing the caller's number before the phone is answered. It discussed the privacy issues, namely the enhanced privacy of those who no longer receive obscene calls, and the reduced privacy of those placing calls. Supposedly it is "a potent deterrent that already seems to have sharply reduced those annoyances [crank calls] in New Jersey."

Then it mentioned Call Blocking, an added feature not available in New

Jersey, but to be available for free in California:

``By pressing two or three keys, callers could keep their numbers from being transmitted. The recipient would not see the number on the screen, only a 'P' [what do you suppose 'P' stands for?] or some other symbol. Like an apartment dweller who sees that the front door peephole has been blocked, he could simply decline to respond to the call. The trouble with Call Blocking is that it undermines Caller ID. Why would people buy Called ID if it could be so easily defeated?"

The answer is easy: they would for the same reason they install peepholes--they will know when it is being defeated.

The editorial goes on to distort the balance of privacy issues:

``Three privacy interests intersect here. It is difficult choosing between two--the interest of the recipient of calls who wishes not to be harassed and the interest of the caller who wishes no to be identified. The third interest, however, might be overriding: society's interest in discouraging offensive phone calls generally."

Simply repeating one side of the argument twice (from an individual and a societal point of view) does not make it carry twice the weight.

The editorial concludes that a bill sponsored by Sen. Herbert Kohl to require free Call Blocking should be defeated, until the impact on privacy of Caller ID with and without Call Blocking can be measured.

I wrote a response to the editor, which concludes:

Even without Call Blocking, those wishing to harass could do so anonymously from pay phones. But this might be too much discouragement for those wishing to place anonymous calls to crisis hotlines, as you suggest. Of course the organizations running those hotlines can probably be trusted not to use Caller ID to trace their calls. But people considering placing such calls need all the encouragement they can get to go ahead without fear of identification.

The real danger to society in Caller ID comes from the ability of large companies to maintain databases by phone number. It will be convenient if corporations can quickly identify and service their regular customers by looking up the phone number when a call comes in. But one might wish to make a call inquiring about some product without running the risks of receiving follow-up calls or being placed on a related mailing list.

Call Blocking provides the perfect solution. While private individuals with Caller ID would refuse blocked calls if they feared harassment, I am sure that even those corporations that made use of a phone database would be willing to accept some anonymous inquiries.

Although the drop in obscene phone calls is easy to measure, the risks to callers' privacy are much harder to quantify.

I sense that you do not even plan to measure them at the end of the experiment you propose, in which New Jersey will be the guinea pig.

John M. Sullivan Princeton Univ. Math Dept. [sullivan@math.princeton.edu](mailto:sullivan@math.princeton.edu)

## ✂ Defeating answering machine security codes

Denis Coskun <dcoskun@alias>

Fri, 9 Feb 90 20:21:00 est

In [RISKS-7.69](#) Vince Manis tells us that his General Electric answering machine has only 256 possible access codes for remote message retrieval. I have the same machine. Valid combinations are 3 consecutive touch tones of the form [0-7][0-7][0-3].

In [RISKS-7.73](#) William Curtiss points out that most answering machines just ignore digits until you get the correct security code. "As long as the incoming stream contains the code somewhere you are given access. Since 256 combinations needs three digits, a carefully constructed string of 258 digits will contain every possible combination (for example, if the code is a triplet composed of just the numbers 1 and 2 then the string 1211122212 contains all eight triplets)."

The shortest string of digits that I was able to generate for defeating my answering machine was 452 digits:

```
000100200301101201302102202303103203304004104204305005105205
306006106206307007107207311121131221231321331401411421431501
511521531601611621631701711721732223233240241242243250251252
253260261262263270271272273330034034134234335035135235336036
136236337037137237344044144244345045145245346046146246347047
147247354054154254355055155255356056156256357057157257364064
164264365065165265366066166266367067167267307407417427437507
51752753760761762763770771772773
```

DTMF decoding chips are required to recognize a tone as short as 50 milliseconds with an interdigit interval of another 50 milliseconds, making a total of 100 ms for each digit. So the whole 452 digit string could be dialed within 45.2 seconds using a demon dialer. Since my answering machine will wait a minute or more while you leave a message, it could be cracked with just one phone call.

Can anyone suggest an algorithm to generate a shorter string than I have above, or better yet, an optimal string? A string length of 258 digits is a lower bound, but is there necessarily a solution that short?

I checked more than a dozen different answering machines on the market that allow remote message retrieval using touch tones, and the best let you select combinations of the form [0-9][0-9][0-9]. A key space of 1000 combinations is hardly any improvement.

Denis Coskun dcoskun%alias@csri.utoronto.ca utcsri!alias!dcoskun

---

## # How to make answering machines deliver ransom messages

*Fri, 9 Feb 90 20:22:57 est*

I discovered a security weakness that would allow you to trick answering machines with remote message retrieval into making phone calls and delivering untraceable ransom messages!

Here's how:

Dial someone's answering machine and leave a message with the format:

1. 14 seconds of nonsense talking (to keep the tape running)
2. dial, say, 555-1234 using touch tones (which will be recorded)
3. a few more seconds of random talking
4. finally your ransom message

Now dial the security code (which you discovered as described in my companion article) to get the answering machine to play back the messages. As soon as you hear the start of your nonsense message, hang up. The machine will continue playing the messages, oblivious to the fact that no one is listening. The telephone exchange will supply dial tone to the answering machine's line 12 seconds after you hang up (12 seconds at my exchange). Two seconds later, the answering machine will play the recorded touch tones 555-1234, effectively dialing that number. A few seconds later, the person at 555-1234 answers and your message is delivered! And it cannot be traced to you.

Of course, you would call back the answering machine and clean up the evidence.

I believe that the technique will work on all answering machines with remote message retrieval provided that:

1. You have the security code (see my other posting about how good these are).
2. The exchange will supply dial tone to the callee after the caller hangs up. This is true on all modern switches.
3. The phone line of the answering machine permits touch tone dialing. This is a way to secure your answering machine: switch to pulse dialing only service.
4. The machine and its tape reproduce touch tones with enough fidelity. Mine do.
5. The machine will ignore dial tone. There are no guaranteed electrical changes on the line when a caller hangs up, so watching for dial tone would be the only reliable indicator, which my machine ignores.

6. The machine will record touch tones. Mine will record everything (except that the 3 digit security code gets it to play back the messages). The security hole could be plugged if the machine would stop recording as soon as it got any touch tone.

7. The machine will play all touch tones recorded on its tape. I did have some trouble here since the machine cannot tell if a tone is coming from the tape or from the caller on the line. During playback, my machine will interpret a "1" as a command to fast forward and "3" to fast reverse, and thus disrupt the dialing if these digits are part of the number.

A more likely hazard than untraceable ransom messages is the relaying of long distance messages that are charged to some innocent answering machine owner, or harassing the owner by having him billed for random toll calls (long distance, overseas, 976, 900, etc.).

Denis Coskun dcoskun%alias@csri.utoronto.ca utcsri!alias!dcoskun

---

## **✶ More on the Hubble Space Telescope**

*Hank Strub <strub%coqsci@ucsd.edu>*

*12 February 1990 0909-PST (Monday)*

The 2/11/90 New York Times Magazine has a long article on the space telescope. This article goes into some detail on the project's software problems

"...scientists were aiming for a 1985 launching, but because so much of the technology related to secret military systems, the Pentagon dictated that only 116 managers in the project could have access to the contractors' plans. 'This lack of manpower came back to haunt us many times,' Robert O'Dell, who now teaches at Rice University, wrote in Sky & Telescope magazine last July. 'It kept NASA from closely following the contractors' work and made it very difficult to know what was happening at any given time.

Costs soared and deadlines were missed. The system that controls the telescope's directional pointing encountered difficulties, which made matters worse. Only after a management reshuffling at Marshall Space Center, and the addition of more overseers, did the project finally get back on track, but with launching delayed until late 1986."

The article continues explaining problems that resulted from launching the telescope from the shuttle to a 380 mile orbit instead of to the originally planned on 22,300 mile equatorial orbit. Leading into:

"Rodger Doxsey, chief of engineering support for the space telescope institute, concedes that the delay caused by the Challenger disaster was not all bad: 'We were not ready to operate the telescope in 1986. There would have been a big scramble just to get it operating. But that's a route history didn't take.'

The biggest problem was in developing the computer software

to control the constantly orbiting telescope: slewing it into position, pointing it to targets and keeping them in the field of view, making adjustments dictated by the interference of Earth and the need to avoid looking at the Sun. (To prevent damaging glare to the optics, the telescope cannot point within 20 degrees of the bright limb of Earth or within 50 degrees of the Sun.) Computers also instruct the telescope about which cameras or sensors to operate for a particular observation, and which of the many camera filters it should use. The computer must then schedule a time when the resulting data can be radioed to Earth through the two tracking and data relay satellites, which are not always available, because of commitments to shuttle missions and various spy satellites. Each observation, whether for a few hours or several days, must be meticulously planned down to the second. 'The entire architecture for this software has had to be very much redefined in the last four years,' Doxsey says."

Hank Strub      hbstrub@ucsd.edu    hbstrub@ucsd.bitnet  
Cognitive Science  
UCSD, D-015  
La Jolla, CA 92093-0515    (619) 534-2541

---

### **✶ Human blamed, not the computer! -- jury duty**

*"Lee S. Ridgway" <RIDGWAY@mitvma.mit.edu>  
Mon, 12 Feb 90 13:02:49 EST*

Last week I fulfilled one of my civic obligations by complying with a summons for jury duty - which meant showing up at the appointed time and place, in order to sit and wait until called or dismissed. [This on the same day the Commonwealth announced it would file misdemeanor charges against no shows. But I digress.]

In Massachusetts, you are called to serve one day or one trial. The one day is covered by sitting in the jury assembly room, waiting. Once the one-day / one-trial obligation is met, you are not supposed to be summoned again for three years.

In the introductory remarks given by the jury clerk, he admonished us to stash our certificate of service in a safe place, because it will be the only sure-fire proof that we did, indeed, do our duty. He continued, and I quote, "SOMEONE did something to the computer, and so a lot of people who should not be receiving jury summonses are - sometimes monthly..."

I was struck by the fact that the clerk did not blame the computer for having messed up the records of who was eligible for a summons and who wasn't, that he blamed it on a human. And this was a person who, although articulate, would not normally be thought of as terribly concerned with such fine distinctions.

---

### **✶ Accents are more than just decorations**

*Kai-Mikael J{{-Aro <d85-kai@nada.kth.se>*

*Tue, 13 Feb 90 10:10:17 +0100*

Accents are more than just decorations

The ASCII character set has (obviously) been developed by Americans for Americans. This is all very well, but since most nations use American computers they, too, get to use the ASCII character set. One consequence of this is that one gets into problems when trying to display characters not present in the original ASCII set. What has been done, then, in most instances is the replacement of certain less commonly used characters, mainly [\]{}}, with "national" characters.

But this isn't problem-free. One thing soon noticed is that even though the characters display as letters on the screen, they are still by most programs interpreted as non-alphabetic to the confusion of (not exclusively) novice users. This also means that programming languages which use these special characters, C is a prime example, look strange, to say the least, when displayed with national characters.

Another problem that soon crops up is that of sort sequence. Most languages treat accented characters as letters with decorations, thus acute, agrave, acircumflex and so on, all count as a's. However, in the Nordic languages the situation is somewhat different. Aring, Adieresis and Odieresis in Finnish and Swedish, and their Danish and Norwegian counterparts Aring, AE and Oslash count as actual letters - thus they have an alphabetic order of their own. To further complicate the matter, this order isn't the same in the different languages - Finnish and Swedish have ...X Y Z Aring Adieresis Odieresis while Danish and Norwegian has the order ...X Y Z AE Oslash Aring. In spite of this, the decision was taken to use the same order in all four countries and the Danish/Norwegian order was chosen.

This means that when you sort something alphabetically in Swedish, all words containing Aring will end up in the wrong place. If they end up at all, that is to say - a few years ago I read in the newspaper that the literary magazine BLM had failed to send out any issues to subscribers who's name started with Aring. This was blamed on "computer error", but a little afterthought gave the realization that some programmer had used a test like  
if ch >= 'A' and ch <= 'Odieresis' then ...  
and thought he had handled the entire alphabet.

Eight-bit character sets solve the problem of displaying both national characters and braces/brackets but they generally don't solve the problem with different sort orders.

There are then some added complications:

At least in Swedish, V and W are considered to be equivalent, thus "Walle" comes before "Ville" in a sort.

The Aring has been introduced in Danish and Norwegian very lately, as a replacement for the Aa-digram. However, proper names are still

often spelled with aa, and thus aa and aring have to be sorted as if they were equivalent, but then again, there are foreign words that contain the combination aa, and these are to be sorted as if they had two a's in a row, so one would get "(den) Haag", "H<aring>b", "Haagerup". This is probably not very easily done on a computer...

Kai-Mikael J{{-Aro (d85-kai@nada.kth.se)  
^^These are adiereses

Thanks to Mogens Lemvig Hansen for explaining the Danish alphabet to me.

---

### ✦ [Parse-ly, Rosemary, Time, Light, Control & Other SAGE Remarks]

*"Martin Minow, ML3-5/U26 12-Feb-1990 1023" <MINOW@BOLT.enet.dec.com>  
Mon, 12 Feb 90 07:30:09 PST*

(Comments on various postings in [Risks 9.67](#).)

Les Earnest's memoir of SAGE reminded me of a story told by a high-school buddy who went into the Air Force before college. He ended up as a technician at a SAGE installation. As Les relates, SAGE used a dual-processor system for reliability: one online, one offline for testing.

One day, the officer in charge stepped out for coffee. The technicians switched to the other cpu and started running diagnostics on the system that had been online. One of these diagnostics turned on all lamps to check whether any were burned out. The officer then came back with a cup of coffee, glanced at the system he thought was defending America and decided that the Hour Of Destiny had arrived. The coffee cup was tossed aside as he left to battle stations. The next day, as my friend related, a very prominent "ON LINE" sign was added to the system.

My friend also mentioned that the graphics system could be used to display pictures of young women that were somewhat unrelated to national defense -- unless one takes a very long view -- with the light pen being used to select articles of clothing that were considered inappropriate in the mind of the viewer. (Predating the "look and feel" of MacPlaymate by almost 30 years.) Perhaps Les could expand on this; paying special consideration to the risks involved in this type of programming.

....

The discussion of whether the Vincennes' missile control system must obey "rules of engagement" brings up an interesting problem that has no simple solution: who is in charge of the technology? To simplify the problem somewhat, should the engine control computer in my car allow me to drive faster than 55 miles per hour? Should I reprogram that computer when I enter an Interstate highway or ship the car to Germany?

A few years ago, I was one of the developers of the DECTalk speech synthesizer. I took some care to make sure that the most common English obscenities were

properly pronounced. One of my goals with DECTalk was to build a tool that could be used by a speech-impaired person and I felt that, no matter how improper the language, it was not my job to restrict the user's expression.

The purpose of a missile control computer is to kill people. It strikes me as bizarre to require the computer program to obey international law as well. Why should a machine be held more -- or even as -- responsible than the ship's captain?

....

In Scandinavia, car headlights are to be kept on 24 hours per day. The local manufacturers have added relays to shut the headlights off when the ignition is turned off. This seems both simpler and more effective than buzzers and synthesized voices. Of course, this is technology being used to aid compliance with the law.

....

When I started this note, I thought I was commenting on three unrelated topics. Apparently, everything is related.

Martin Minow

---

### **✂ Blazers (Re: Woodhead, [RISKS-9.67](#))**

*Jeff Berkowitz <jjb@sequent.uucp>  
11 Feb 90 17:24:49 GMT*

Robert J Woodhead writes:

>Fortunately for many of us, after about 40 years of intense debate in the  
>automotive industry on this complex and challenging "lights on" problem, some  
>manufacturers are adding a simple device that alerts you if your lights are on  
>when the ignition is off. These range from a simple analog "BReeee!" in my  
>Chevy Blazer...

I have a Blazer (actually a GMC Jimmy, the same vehicle) with the "analog BReeee!" feature referred to by Mr. Woodhead. I won't disagree that the buzzer is a nice feature. The observed rate of "battery dead due to lights on" with this vehicle, however, is higher than any other vehicles we have ever owned (two occurrences in 18 months).

The problem is caused by a small convenience light located on the ceiling of the vehicle just inside the rear cargo compartment door. The light housing includes a rocker switch, which requires very low pressure to operate and is aligned axially rather than longitudinally. The switch is therefore easily operated by accident. The act of lifting a grocery bag from the rear compartment can cause the lip of the bag to move the switch, for example.

This tiny light is NOT coupled into the manufacturer's "beeper system", of course - that would be too annoying. The light is very faint, so faint that one can fail to observe it when peeking into the garage at

night. We believe that about three days of continuous operation of the light are sufficient to drain the battery to the point that it will not start the car (we're not sure about this, since we never really know when the switch was thrown as we scurry around, days later, connecting jumper cables :-).

To my mind, this is an excellent "microexample" of how a complex system design can fail miserably to achieve the intent of the designer. Although this system is not computerized, it contains an obvious message: reliability can't be glued on.

Jeff Berkowitz N6QOM      uunet!sequent!jjb  
Sequent Computer Systems      Custom Systems Group

---

**✂ Re: Computers, good and evil (Sicherman, [RISKS-9.67](#))**

<gateh@CONNCOLL.BITNET>  
Fri, 9 Feb 90 10:29:41 EST

> "Apple pie is in itself neither good nor bad; it is the way it is used..."

I have read none of the works on this topic, but (unless I am thoroughly confused) it seems that McLuhan's apple pie analogy is a somewhat sarcastic attempt at supporting his argument that technologies (and apple pie) do have inherent qualities or a "nature" which renders them "good or bad" of their own. Apparently he feels that the "nature" of apple pie is good, and

Certainly he could not infer such a quality unless he liked apple pie, something which is obviously not true for all people. In fact, for those allergic to apples, the nature of apple pie is, if anything, bad. And so he has succeeded in proving the very point made by Sarnoff.

Gregg TeHennepe                      | Minicomputer Specialist  
gateh@conncoll.bitnet                | Connecticut College, New London, CT

---

**✂ Telephone Switch Security**

Roland Ouellette <rouellet@polaris.cs.uiuc.edu>  
Mon, 12 Feb 90 19:36:28 CST

Lately there has been little lack of discussion about reliability of telecommunications systems. I have also seen several articles which discuss the security of the same systems. MIT has recently installed an ISDN system using a #5ESS system. There has been a whole lot of discussion about what the system can and cannot do. October '89's issue of Technology Review has an article entitled "The Twilight Phone." In February's issue there is an editorial and two replies.

The editorial claims that it is possible to use the phone system to bug rooms. The replies claim that, while theoretically possible, getting the switch to do that would require programming expertise and

physical access to the switch.

There then is the possibility that folks in charge could order the owners of the switch to bug a room. This is more invasive than a normal wire tap, because the phone's microphone could be left on all of the time.

Then there is this article which appeared in the WSJ. It does not state how said hackers "entered the company's computer," but it makes me wonder. I'd be interested to hear how these calls were rerouted.

Hackers - Accused of scheme against BellSouth. Legion of Doom group.  
{The Wall Street Journal, 8-Feb-90, p. C20}

Federal grand juries in Chicago and Atlanta indicted four alleged computer hackers in what authorities called a fraud scheme that could potentially disrupt emergency "911" telephone service throughout nine Southern states. The men, alleged to be part of a closely knit cadre of computer hackers known as the Legion of Doom, gained access to the computer system controlling telephone emergency service of BellSouth Corp., the Atlanta-based telecommunications giant. The Chicago indictment said members of the Legion of Doom are engaged in disrupting telephone service by entering a telephone company's computers and changing the routing of telephone calls. The hackers in the group also fraudulently obtain money from companies by altering information in their computers, the indictment said. The hackers transferred stolen telephone-computer information from BellSouth to what prosecutors termed a "computer bulletin board system" in Lockport, Ill. In turn, the men planned to publish the computer data in a hacker's magazine, the grand jury charged.

Roland G. Ouellette rgog1070@uxa.cso.uiuc.edu rouellet@babym.cs.uiuc.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 9: Issue 69**

**Tuesday 20 February 1990**

## Contents

- [A320 accident](#)  
[Nancy Leveson](#)  
[George Michaelson](#)
- [Ferry line replaces "sail-by-wire" with pneumatic controls](#)  
[Jon Jacky](#)
- [Now Prodigy Can Read You](#)  
[Donald B Wechsler](#)
- [3 KGB Wily Hackers convicted, mild sentences](#)  
[Klaus Brunstein](#)
- [Problems/risks due to programming language, stories requested. \[Item Includes AT&T "do...while"..."switch"..."if"..."break" tale\]](#)  
[Gerald Baumgartner](#)
- [AT&T Says New Goof Wiped Out Many Toll-Free Calls](#)  
[David B. Benson](#)
- [Re: Computerized Collect Calls](#)  
[Adam Gaffin via Mark Brader](#)
- [RISKS of ANI blocking](#)  
[James C Blasius](#)
- ["Brilliant Pebbles"](#)  
[Gary Chapman](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **A320 accident**

*Nancy Leveson* <[nancy@murphy.ICS.UCI.EDU](mailto:nancy@murphy.ICS.UCI.EDU)>

*Wed, 14 Feb 90 12:09:11 -0800*

>From the AP wire: by Sharon Herbaugh, Associated Press Writer,

NEW DELHI, India (AP) - An Indian Airlines jet with 146 people aboard crashed and burst into flames while attempting to land at a southern Indian airport today and 91 people were killed, authorities said. The Airbus 320 crashed at 1 p.m. while on final approach to the runway at Bangalore airport, airline and airport officials said. The plane apparently grazed a grove of trees and

crashed about 50 yards from the runway, they said.

State-run television showed shots of the crash site, a grassy plain on a golf course adjacent to the airport. The craft's tail was intact, but its fuselage was shattered and charred and the nose smashed. "The crash occurred before the plane touched the runway, and it caught fire as soon as it crashed, said P..S. Ghetty, airport manager in Bombay, where the hourlong flight had originated.

The crash was the first by the sophisticated Airbus 320 on a commercial flight. One of the planes crashed in a demonstration flight at an airshow in eastern France in 1988 killing three people and injuring 50. Airline officials said the plane, which was an hour behind schedule, carried 139 passengers and a crew of seven.

[More about injuries]

Airline officials did not know what caused the crash, but they said weather was not a factor. The jet was acquired by the nation's government-run domestic carrier about three months ago for \$38 million.

After Indian Airlines announced it was adding 31 Airbus 320s to its aging fleet of Boeing, Fokker, and Avro planes, news reports criticized the airline for failing to adequately train pilots to fly the sophisticated aircraft, the first civilian airliner with a fully computerized flight control system. The carrier also was criticized for failing to provide adequate hangar space to house and maintain the planes.

[more about some previous Indian Airlines accidents]

Indian Airlines, the major domestic carrier, flies to 73 cities nationwide and to nine nearby countries. It has come under criticism for allegedly failing to maintain pre-flight safety procedures on its fleet and to adequately supervise its pilots. Delays in flight schedules are also endemic.

The A320, built by the European consortium Airbus Industrie, is the first civilian airliner equipped with a fully computerized flight control system, which the manufacturer says permits safer, electronically controlled flight. Developed at a cost of nearly \$2 billion, the A320 was certified for flight on Feb. 26, 1988, and went into service in April 1988.

[There have also been some unofficial radio reports that suggested that the flight control system was involved in this crash. My friends in the industry say that this cannot possibly be known for a while. nancy]

[Also noted by Robert Dorsett (rdd@rascal.ics.utexas.edu)  
and David B. Benson (benson@cs2.cs.WSU.EDU), Steve Milunovic  
<Steve\_Milunovic@quikmail.sri.com>. PGN]

---

**✶ yet another A320 problem**

*George Michaelson <ggm@cc.uq.oz.au>  
Thu, 15 Feb 90 16:39:16 +1100*

[...] Doubts were expressed about the ability of the airline to maintain the complex flight control equipment, and the effects of dust on the system, both with explicit reference to computing systems.

I find it hard to raise any possible risks in technology transfer to developing countries (does that label apply to India?) given the overtones of chauvinism if not downright racism, but it seems from this interview as if the Indian engineers themselves question their ability to handle this package.

I suspect other parallels exist with well-meaning donation/supply of IT infrastructure that failed to match local conditions eg lack of tropical "hardening", availability of spike-free UPS, spares, training.

sort-of comp.society but has some RISKy overtones... -George

---

### **✂ Ferry line replaces "sail-by-wire" with pneumatic controls**

*Jon Jacky <JON@GAFFER.RAD.WASHINGTON.EDU>*

*Mon, 19 Feb 1990 20:02:49 PST*

This article appeared in IEEE SPECTRUM, vol 27, no 2, Feb. 1990, page 54:

FAULTS AND FAILURES: FERRY ELECTRONICS OUT OF CONTROL by Karen Fitzgerald with John R. Devaney and Robert Thomas

In a seeming reversal of progress, Washington State Ferries, the agency that manages the United States' largest ferry transportation system, has begun replacing the electronic control systems of six of its boats with pneumatic controls. A string of failures, beginning in the early 1980's after the Issaquah-class ferries were introduced, eventually forced the change. Ferries rammed docks, for instance, or pattered away from them even though no command was given. In a few instances, a ferry shifted from forward to reverse with no warning. In contrast, an Issaquah boat retrofitted last June with a hybrid electro-pneumatic system has outstripped all expectations, according to vessel maintenance engineer Ben Davis.

[ Here the article includes a photo of an Issaquah ferry. They are large, carrying several hundred cars, their passengers, and hundreds of walk-on passengers - JJ ]

As part of the state's Department of Transportation, Washington State Ferries in Seattle operates 24 vessels, encompassing a variety of control systems. No others have had the problems of the six boats in the Issaquah class, which are unique in having variable-pitch propellers, one at each end of the boat. When the captain sets the control handle positions for transit or movement near the dock, the control system must set the appropriate propeller speed, pitch, and clutch engagement. Variable pitch makes the craft extremely maneuverable, able to move sideways and turn on the spot.

Many of the problems could be traced to the vendor, Propulsion Systems Inc. (PSI), which went bankrupt in 1981 and was then bought by the ferry builder, the now-defunct Marine Power and Equipment Co. "The problem is not so much

with digital controls," said Davis, "as with horribly shoddy control system design."

[ Here the SPECTRUM article describes examples, including poor understanding of the propulsion system, grounding and shielding problems, poor protection against power supply dropouts and transients, poor documentation and configuration control, and incorrect assembly ]

... a 1986 Lockheed Shipbuilding Co. study recommended switching to pneumatics to improve reliability. ... The agency chose a hybrid control system that operates electrically from control handles to control cabinet ... but operates pneumatically from cabinet to propellers and engine governors ... (the replacement control system is) supplied by Mathers Control Inc., Seattle. ...

- Jon Jacky, University of Washington (in Seattle)

---

### **✂ Now Prodigy Can Read You**

*Wechsler, Donald B <m17434@mwvm.mitre.org>  
Thursday, 15 Feb 1990 17:11:22 EST*

The Prodigy Services publication, PRODIGY STAR, (Volume III, No. 1) recently showcased a "major benefit". The Prodigy system accesses remote subscribers' disks to check the Prodigy software version used, and when necessary, downloads the latest programs. This process is automatic when subscribers link to the network.

I asked Prodigy how they protect against the possibility of altering subscribers' non-Prodigy programs, or reading their personal data. Prodigy's less-than-reassuring response was essentially (1) we don't look at other programs, and (2) you can boot from a floppy disk. According to Prodigy, the feature cannot be disabled.

---

### **✂ 3 KGB Wily Hackers convicted, mild sentences**

*Klaus Brunnstein <brunnstein@rz.informatik.uni-hamburg.dbp.de>  
15 Feb 90 15:50 +0100*

A court in Celle (a small town near Hannover, FRG) today (Thursday 15,1990) convicted 3 KGB hackers of espionage (=to work for a foreign service against the interests of the country) for the KGB. Sentences were mild and partly significantly below the recommendation of the public prosecutor. Markus H. (whom Clifford Stoll regarded as 'the Wily hacker') was found guilty of having intruded US military computer systems 30 times (out of 450 attempts); his sentence: 20 month prison (for 3 years on probation) and to pay 10,000 DM; Dirk B. was sentenced to 14 months and has to pay back 5,000 DM. And finally, former croupier Peter C. (who essentially connected the links to KGB but has no knowledge in computing) was sentenced to 2 years and has to pay back 3,000 DM. All of them lost the 'citizen rights' (e.g. to participate in elections, either passively or actively) for 2-3 years. The prison sentences are deferred for 3 years probation time. They were immediately released from detention pending

trial.

The chairman of the 2nd senate of the Nether Saxonian Criminal Court said in his oral argumentation, that the Federal Republic didnot suffer seriously from the hack, but that US military institutions and a large manufacturer were damaged. (As the German law has not the same universality as US law, damage tu US instutions couldnot be prosecuted). Moreover, the court expressed strong doubts that a real damage was done: 'only' a security package of a large manufacturer and the source code for a UNIX system were mentioned. (the large manufacturer evidently prepares a civil case). Independent of whether the sentences are accepted and will become valid, the estimations in media about billions DM of damage were rather premature.

It will be interesting to analyse (in the written argumentation) why the court didnot convince the hackers on the hacker attacks (the German penal law recently was updated by a new paragraph on computer espionage which was not applied). The defenders tried (evidently successfully) to show that Cliff Stoll's proofs were insufficient to show that the guy in Hannover (H.) really was the guy whose commands were executed 10,000 miles away. With a court without any knowledge (the chairman asked the hackers more than once: 'What means' questions on e-mail etc), with public prosecutors and with criminalists which evidently lacked the basic knowledge, it may not surprise that the defenders succeeded in put the material in question (Cliff Stoll's book was forbidden to be sold in its German version, due to several statements which the defenders neglected).

I apologize for any misformulations esp. regarding legal language (I am not educated as a lawyer); moreover, I hope that my personal doubts about the competence of the criminal agencies, the prosecutor and the court are not overstated here. On the other side, the 2 hackers (a 3rd one committed suicide last year, and the defenders tried to load all the guilt on him) and the 4th one, 'Pengo' who may face another process (in Berlin), all belonging to the so-called 'Leitstelle 511' (due to the telephone prefix of Hannover) of Chaos Computer Club are not those professionals as they are regarded by the media and the lawyers. Klaus Brunnstein

---

### **✶ problems/risks due to programming language, stories requested**

Gerald Baumgartner <gb@cs.purdue.edu>

19 Feb 90 07:42:16 GMT

[Gerald is collecting stories on the risks of choosing the wrong programming language, including problems that could have been avoided if another (a better) programming language would have been used. He cited the Mariner (but hadn't seen the newer explanations in [RISKS-8.75](#) or [RISKS-9.75](#)), the Internet Worm fingered problem, and the 15 Jan 90 AT&T slowdown. But he included the following text on the AT&T problem. PGN]

>From: kent@wsl.dec.com

| | Subject: AT&T Bug

| | Date: Fri Jan 19 12:18:33 1990

| |

| | This is the bug that cause the AT&T breakdown  
| | the other day (no, it wasn't an MCI virus):  
| |  
| | In the switching software (written in C), there was a long  
| | "do . . . while" construct, which contained  
| | a "switch" statement, which contained  
| | an "if" clause, which contained a  
| | "break," which was intended for  
| | the "if" clause, but instead broke from  
| | the "switch" statement.  
| |

Again it looks like this bug wouldn't have occurred in another programming language.

You C what I mean? Do you know other stories like these, if possible with references? I don't want to praise Ada or pick at C and Fortran; I am looking for any story where a provably inappropriate/insecure programming language has been used.

Gerald Baumgartner gb@cs.purdue.edu ...!{decwrl,gatech,ucbvax}!purdue!gb

---

## ✂ AT&T Says New Goof Wiped Out Many Toll-Free Calls

David B. Benson <dbenson@cs2.cs.WSU.EDU>

Wed, 14 Feb 90 11:36:41 PST

The Wall Street Journal, Tuesday, February 13, 1990

By John J. Keller, Staff Reporter of The Wall Street Journal

New York -- American Telephone & Telegraph Co., still reeling from a crippling network outage less than a month ago, suffered another accident on Friday that wiped out toll-free 800 service to tens of thousands of callers nationwide.

AT&T blamed the latest disruption on a service technician who had forgotten to program some information on a group of 800 numbers into a network computer.

Only companies subscribing to 800 numbers using the prefix 424 were affected, said AT&T. That included the Internal Revenue Service's toll-free, tax-service number 1-800-424-1040. Another IRS line that allows callers to order forms by phone was also cut off.

AT&T declined to identify business and government agency customers other than the IRS that were affected by the Friday shutdown, which lasted about 90 minutes, from 12:40 p.m. EST to a little after 2 p.m.

While that's nowhere near the nine hours that AT&T's network had problems on the afternoon and evening of Jan. 15, it was an embarrassing epilogue to the earlier breakdown. Until the January problem, AT&T hadn't experienced a major network problem in its 114-year history. The January outage was caused by a software programming error in the company's network signaling system.

"AT&T offers the most modern services, but this latest accident was at the lowest level of sophistication," said Jack B. Grubman, an analyst at PaineWebbber Inc. "Thats not good."

The AT&T spokesman blamed Friday's accident, which he called a "very small mishap" and a "minor inconvenience," on a network service technician who was "load balancing" or making network routing changes to some 800 numbers. The technician was supposed to transfer the list of these 800 numbers from one network control point to another, he said. But apparently the technician forgot to program the routing changes into one of the control points, shutting down service on as many as 200 toll-free lines, including those leased by the IRS.

An IRS spokesman said the agency didn't have a clear idea of how many people were affected by the shutdown, but "obviously it was in the thousands. We hope it didn't cause too much of a problem."

---

### **✂ Re: Computerized Collect Calls**

*Mark Brader <msb@sq.com>  
Wed, 14 Feb 90 14:23:01 EST*

On Jan. 7, New England Telephone began switching over to a new computerized system for handling collect calls from touch-tone pay phones. Instead of an operator, you get a computerized voice telling you to punch "one one" for a collect call. Then you say your name, the computer dials the other number, tells the person it's a collect call and then plays you back as you state your name.

Just one problem. One of the reporters where I work was negotiating a sensitive interview and needed to talk to the editor-in-chief. He didn't have any change, so he tried calling collect. Another editor picked up the phone, thought it was one of those "goddamned computer telemarketing things" and promptly hung up.

Adam Gaffin, Middlesex News

---

### **✂ RISKS of ANI blocking**

*James C Blasius <dopey@iwtil.att.com>  
Thu, 15 Feb 90 20:44:34 EST*

AT&T has recently seen fit to start using Illinois Bell ISDN at my location, replacing thousands of individual answering machines (that don't work with digital phones) with an AUDIX answering system.

We have automatic number identification inside the complex, displaying the caller's name on an LCD screen on the phone. We can block ANI when we call somebody, then the name shows up as PRIVATE.

However, if your ANI-blocked call goes to AUDIX, AUDIX leaves your phone number along with your message! Leaves me wondering how much I can trust commercial

ANI blocking if Illinois Bell even offers it.

(The other nifty feature of AUDIX is that it leaves a message of your call even when you don't want it to. Only fix I've found to this is to type \*\*\* and confuse it).

James C. Blasius

---

## ✈ "Brilliant Pebbles"

Gary Chapman <chapman@csl.stanford.edu>

Mon, 19 Feb 90 10:42:30 PST

The San Francisco Chronicle reports today that the Jasons, a group of technically-oriented defense intellectuals who study weapons systems as consultants to the Pentagon, have prepared a report on the "Brilliant Pebbles" program that is highly critical of the concept. Although the report was delivered to the Pentagon last fall after the Jasons' summer study session, the general thrust of the report was not revealed until yesterday, Sunday, February 18, at a symposium at the annual convention of the American Association for the Advancement of Science, being held in San Francisco. A summary of the Jasons' findings was presented by John M. Cornwall, professor of physics at UCLA and a member of the Jasons group. Also part of the symposium was Lieutenant General George Monahan, director of the SDIO.

General Monahan told the audience that it will cost between \$50 and \$60 billion to develop and deploy "Brilliant Pebbles," although others have put the cost at \$100 billion. General Monahan said, "We could have a very robust first-phase defense" with "Brilliant Pebbles." "And the technology is at hand to deploy such a system, so the major considerations now are political."

Cornwall, however, said that the Jasons do not consider the technology to be at hand, and he outlined a number of problems with the "Brilliant Pebbles" concept. He said that the system would be "a somewhat leaky defense," and the "pebbles" would be vulnerable to countermeasures. They would also be ineffective against hostile missiles using fast-burn boosters. Cornwall also reported that the lasers proposed as guidance mechanisms for the projectiles are currently inadequate for the job.

Cornwall concluded, "This design is not ready to be locked into place." He did recommend further support, however, because the system may eventually prove to be a "near-term" possibility. The Bush administration's proposed budget for the "Brilliant Pebbles" program has increased from \$129 million in FY 90 to \$329 million in FY 91.

-- Gary



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 9: Issue 70

Friday 23 February 1990

## Contents

- [Neutron reactor lands in hot water](#)  
[Steve Strassmann](#)
- [Yet another laserwriter health risk?](#)  
[Roy Smith](#) via [Mark Seiden](#)
- [Computer security at stock exchanges vulnerable](#)  
[Rodney Hoffman](#)
- [A320 accident](#)  
[Udo Voges](#)
- [Problems/risks due to programming language \(AT&T Bug\)](#)  
[Jonathan I. Kamens](#)  
[Steve Nuchia](#)  
[David L. Golber](#)  
[Robert L. Smith](#)
- [Re: "Provably insecure programming language"](#)  
[Mark McWiggins](#)
- [Re: Computerized Collect Calls](#)  
[Joseph Beckman](#)
- [What makes a hacker hack?](#)  
[Nigel Voss-Roberts](#)
- [The "Twelve Tricks" Trojan horse](#)  
[Christoph Fischer](#) via [John Rushby](#)
- [Info on RISKS \(comp.risks\)](#)

---

### Neutron reactor lands in hot water

Steve Strassmann <[straz@media-lab.media.mit.edu](mailto:straz@media-lab.media.mit.edu)>

Fri, 23 Feb 90 04:39:28 EST

from New Scientist, 17 Feb 90, page 18

A nuclear reactor at one of Europe's leading physics research centers has been shut down by French safety authorities following the discovery that it had been running at 10 percent over its permitted power output ever since it came into operation in the early 1970's.

The extra power went unnoticed because the instrument used to measure the output of the reactor at the Institut Laue-Langevin (ILL) at Grenoble in France was calibrated with ordinary water, whereas the reactor uses heavy water.

Its reactor generates the world's highest flux of neutrons... .. heavy water is 10 per cent denser than ordinary water. The density term used by the scientists in the equation linking flow with pressure was that of ordinary water. They then poured ordinary water past the diaphragm and observed the relationship between flow and pressure.

"The mistake came in twice; in the equations they used, and in the actual calibration," says Gerard Pautrot, spokesman for the reactor section at ILL. The result was that the power output was systematically underestimated by 10 percent.

Since the uncertainty in calculating the rate at which the uranium is burned is also around 10 percent, the operators of the reactor never noticed that the fuel was burning faster than expected, says Pautrot.

It will not be necessary to alter the data that scientists have obtained with the beam, which is monitored independently. The error was found only when engineers who were trying to improve the system re-examined the old calibration procedures and noticed the error.

---

### **✂ yet another laserwriter health risk?**

*Mark Seiden <mis@Seiden.com>  
Wed, 21 Feb 90 10:58:43 EST*

Originally-From: roy@alanine.phri.nyu.edu (Roy Smith)  
Newsgroups: bionet.sci-resources,sci.research  
Subject: Warning: NIH font size nit-picking  
Date: 20 Feb 90 23:02:08 GMT

One of our faculty members had a grant administratively rejected by NIH because, claims NIH, the guidelines for type size had been violated. They specify 10 to 12 point type, no more than 15 characters per inch. This grant was done using troff, in Times Roman 10 on an Apple LaserWriter, which is what most grants around here get done in. Turns out, however, that Times Roman 10 gives you an average of about 16-1/2 characters per inch.

Apparently somebody at NIH sits there with a ruler and counts characters. I suppose one could debate at length the wisdom of being so finicky about this, but the important thing is that they are, and people should be aware that they do take this seriously and size their type accordingly. OBTW, they did agree to accept the grant for the same deadline if we would print it out again in a larger size and get it back to them in a couple of days, so I guess they are being reasonable about this.

Roy Smith, Public Health Research Institute  
455 First Avenue, New York, NY 10016  
roy@alanine.phri.nyu.edu -OR- {att,philabs,cmcl2,rutgers,hombre}!phri!roy

---

### **✂ Computer security at stock exchanges vulnerable**

Rodney Hoffman <Hoffman.ElSegundo@Xerox.com>  
23 Feb 90 07:57:46 PST (Friday)

Here is a short AP item from the 'Los Angeles Times' 21 Feb. '90:

#### COMPUTER SECURITY AT STOCK EXCHANGES CALLED VULNERABLE

Internal security weaknesses of stock exchange computer systems raise risks of sabotage that "could literally bring securities trading to a halt," even though the systems are well protected against attack by outsiders, a congressional study disclosed Tuesday.

The study by the General Accounting Office found a number of internal control weaknesses at the computer centers of the nation's two major stock exchanges and the National Assn. of Securities Dealers, which oversees the over-the-counter market.

A related GAO study called for beefed-up security measures for the electronic funds transfer systems used by the Federal Reserve System and most of the nation's banks.

---

#### ✶ A320 accident

Udo Voges <voges@idtva.UUCP>  
Fri, 23 Feb 90 08:49:07 +0100

Crash due to stress? Airbus-Copilot had training problems  
(translated from Badische Neueste Nachrichten 22 Feb 90)

Toulouse (dpa). The crash of the Indian Airbus A320 during landing at Bangalore is possibly due to an unqualified pilot, reports the French Newspaper "Depeche du Midi" of Toulouse. The copilot C. A. Fernandez has shown problems during stress situations during his training on a simulator at the training company Aeroformation in Toulouse, the paper reports on Wednesday (21 Feb 90 uv). Therefore the instructors have not given him the qualification certificate and have decided to require an extended basic training in India. The pilot S. S. Gopujkar was probably acting as an instructor during the accident flight on last Wednesday (14 Feb 90 uv), despite the fact that he didn't have the required qualification. This would explain, why he asked the control tower to make a manual landing on sight. The president of Aerospatiale SA, which is part of the Airbus consortium, announced yesterday (21 Feb 90 uv), that the crash had no technical causes, according to existing information. (end of translation of the article)

So again it is - only - human malfunctioning (insufficient training, bad management procedures, financial reasons ?). Udo Voges

---

#### ✶ Problems/risks due to programming language, ... ([RISKS-9.69](#))

Jonathan I. Kamens <jik@pit-manager.MIT.EDU>

Wed, 21 Feb 90 11:35:27 -0500

| | In the switching software (written in C), there was a long  
| | "do . . . while" construct, which contained a "switch" statement, which  
| | contained an "if" clause, which contained a "break," which was  
| | intended for the "if" clause, but instead broke from the "switch" ...  
Again it looks like this bug wouldn't have occurred in another  
programming language.

I have to disagree strongly with the assertion that this bug wouldn't have occurred in another programming language. The bug in question is a programmer error, not a language error, and therefore the same programmer could just have easily made some other programming error in another language.

To quote from K&R 2nd Ed, "A break statement may appear only in an iteration statement or a switch statement, and terminates execution of the smallest enclosing such statement; control passes to the statement following the terminated statement." I don't see anything in there about if statements, and it seems to me that an attempt to use break to exit from an if statement is just a stupid programming error, not a language flaw.

There is some merit to the claim, "Well, a better language would not have allowed such a mistake," but not much (merit, that is). All programming languages have room for stupid errors of one sort or another, or at least all of the ones that are widely used in industry do. I think we're opening a real can of worms when we start blaming the language for something that is the programmer's fault -- if we can't expect our programmers to understand the language with which they are programming, then what \*can\* we expect?

Jonathan Kamens, IT Project Athena

Office: 617-253-8495

---

### ✂ Problems/risks due to programming language, ... ([RISKS-9.69](#))

Steve Nuchia <[steve@nuchat.UUCP](mailto:steve@nuchat.UUCP)>

21 Feb 90 15:21:47 GMT

Presumably the break was intended for the do..while construct, not the if. In any case the problem is generic, and often arises when modifying previously correct code, for instance to handle a new special case.

> Again it looks like this bug wouldn't have occurred in another  
> programming language.

Hogwash. This is the silver bullet fantasy, a RISK in itself when held by practicing programmers. C's break is simply a restricted form of GOTO, and GOTOs with the wrong target are a common error in every language that has GOTOs. That is, every language that would be considered for "serious" applications like switching systems.

Several languages have a break construct that accepts a numeric argument to indicate how many levels to break out of. Rather than eliminating this kind of

error, they offer it increased scope. There is no silver bullet.

Steve Nuchia      South Coast Computing Services      (713) 964-2462

---

**✂ AT&T Bug - should have used a go to**

*David L. Golber <dgolber@aerospace.aero.org>  
Wed, 21 Feb 90 08:15:28 -0800*

I've always found "break" a bit confusing. In this case, I would guess that the programmer knew exactly where he wanted to break to ... that is, what the next statement executed after the "break" statement should have been. I suggest that writing a "go to" might have been more appropriate. (Shocking, but true.)

Dave Golber

---

**✂ re: Problems/risks due to programming language ...**

*Robert L. Smith <rlsmith@mcnc.org>  
Thu, 22 Feb 90 17:43:36 EST*

Mr. Baumgartner:

I'm very surprised that you didn't take, as your principal example of an error suggested by the programming language, the requirement in C to use one equal-sign (=) for a replacement but two of them (==) for a comparison. There have been countless instances of programmers using two when one was meant and, more commonly, one when two were meant, as in an "if" statement. Because it's perfectly legal in C, in an "if" statement, to do a replacement and a comparison at once, the compiler never complains if you use only one equal-sign there. An unintended replacement can be a subtle bug indeed!

The true reason for my response to your query, however, is my objection to the characterization of "break" misuse as a fault suggested by the language. You didn't look deeply enough. The real problem is the contortions forced upon the C user to render his code in holy STRUCTURED format.

If the AT&T programmer had coded "goto" instead of "break", he would have likely had a problem with his peers but none with the machine.

Regards, rLs

---

**✂ Re: "Provably insecure programming language"**

*Mark McWiggins <mark@intek01.UUCP>  
21 Feb 90 17:36:59 GMT*

gb@cs.purdue.edu (Gerald Baumgartner) writes:

> ... I don't want to praise Ada or pick at C and Fortran; I am looking for  
>any story where a provably inappropriate/insecure programming language has  
>been used.

Provably insecure programming language: any such language used by a human being. I don't want to praise Ada either.

Mark McWiggins, Integration Technologies, Inc. (Intek) Bellevue WA 98004  
Address: 1400 112th Ave SE #202 Phone: +1 206 455 9935

---

### **✂ Re: Computerized Collect Calls**

<Beckman.RESORT@DOCKMASTER.NCSC.MIL>

Wed, 21 Feb 90 07:34 EST

What is to prevent someone from abusing a computer taped & delivered 'name'?

COMPUTER: Please state your name.

CALLER: Hi Mom, I'll be home tomorrow on flight...

COMPUTER: (After dialing number) Will you accept a collect call from  
"Hi mom, I'll be..." If you wish to accept charges, please say "yes,"  
otherwise say "no."

CALLEE: No.

COMPUTER: Thank you. (And does not charge anyone for the message just  
forwarded.)

Does anyone know how long of a "name" will be accepted? How about if modem  
tones will be accepted, stored & relayed if given during the "name" period?

Joseph [Also noted by amos@nsc.UUCP (Amos Shapir)]

---

### **✂ What makes a hacker hack? (BBC World Service program)**

Nigel Voss-Roberts <robertsn@iosg.enet.dec.com>

Thu, 22 Feb 90 11:41:11 PST

"The Multifaceted Hacker"  
or "What makes a hacker hack?"

I'd like to enlist the assistance of the RISKS community in defining the many  
different faces of what a hacker is (in any and all senses of the word).

A good friend of mine, Rossella Str<0">m, is researching this subject for a BBC  
World Service radio documentary. She intends to explore the subject what she  
hopes will be a new and different angle, and one that I hope RISKS readers  
would regard as more accurate. You could help make it so.

As an illustration, newspapers & the rest of the media first picked up on the image of the "Boy Wonder Hacker", prepubescent geniuses writing sophisticated computer programs instead of playing football like other kids.

Then they picked up the image of the "Wily Hacker", the cyberpunks on the Dark Side, breaking into military computers and selling secrets to the men in black hats for drugs and money.

Some of us, of course, would have preferred the world to recognise the old-fashioned cosy image of the hacker as a clever programmer, or someone who is good with train sets. (This could be your last chance to help revive the traditional meaning of the word)

All of the above are true to some extent. None of the above completely define "The Hacker Phenomenon" (whatever that really is).

What Rossella is looking for is information on the human side of what being a hacker is. What makes some people spend long hours working on clever programs for their own sake; what makes some people see unauthorised access to computers as a game?

In other words, CHARACTERISTION and MOTIVATION.

I have of course recommended the following books to her as a starting point.

"Computer Power & Human Reason" by J. Weizenbaum

"Hackers" by S. Levy

"The Cuckoos Egg" by C. Stoll.

But I'm sure there's much more to it than that and I believe that RISKS readers are a unique group to ask this question.

I'm sure that many readers of RISKS would be interested in your replies, but if you do have any insights which you don't want to send to the general distribution, then you can contact Rossella in complete confidence by mail at the following address:

Postbus 597, NL - 2131 BA Hoofddorp, The Netherlands.

or through me. Thanks. Nigel Roberts. Tel: +44 860 578600 or +44 206 396610  
Fax: +44 206 393148

---

### **✂ The "Twelve Tricks" Trojan horse (for whoever hasn't seen this)**

*John Rushby <RUSHBY@csl.sri.com>*

*Mon 12 Feb 90 21:23:00-PST*

>From: RY15@DKAUNI11.BITNET (Christoph Fischer)

Newsgroups: comp.binaries.ibm.pc.d

Subject: The "Twelve Tricks" trojan - alert and description

Message-ID: <KPETERSEN.12565845400.BABYL@WSMR-SIMTEL20.ARMY.MIL>

Date: 12 Feb 90 21:31:29 GMT

## The "Twelve Tricks" trojan - alert and description

We have recently received and analysed a trojan that we believe warrants an urgent alert. We are calling it the Twelve Tricks trojan, and it is very interesting, very nasty, and quite complex. This message is not meant to be a complete description of the trojan - we feel that it is important to get a warning out quickly, rather than aim for completeness. It is not a virus.

The trojan consists of a program (more about this aspect later) which you run; running the program, as well as the obvious things that the program is expected to do, also replaces the partition record (also called the Master Boot Record, or MBR) on your hard disk with its own version. This can easily be recognised by inspecting the hard disk at cylinder zero, head zero, sector one, which can be done with a disk sector editor such as Peek-a. If the partition has this trojan in place, it will contain the following text near the beginning:

```
SOFTLoK+ V3.0 SOFTGUARD SYSTEMS INC  
2840 St. Thomas Expwy,suite 201  
Santa Clara,CA 95051 (408)970-9420
```

At this point, let us state that we believe that the company mentioned above has nothing whatsoever to do with the trojan; perhaps the trojan author has a grudge against them.

The trojan uses a far call to the hard disk Bios code in order to plant this partition. To do this, it must know the location in memory of the entry point; it tries five different ones, one of which is the one documented in the IBM PC-XT Technical reference manual, and the other four are presumably fairly common alternatives.

The purpose of planting the trojan with a far call is, we believe, to escape detection by Active Monitor programs that protect a computer by monitoring the interrupt table, and preventing unauthorised writes to system areas on the hard disk. Since Twelve Tricks doesn't use an interrupt to plant the MBR, such programs won't be able to prevent it. We tested this using Flushot+, probably the most successful of the Active Monitors, and Twelve Tricks went straight through it - the same would be true, we think, of any other Active Monitor.

## The Replacement MBR

When the MBR is run, which is every time you boot from the hard disk, Twelve Tricks copies 205 (d7h) bytes of itself onto locations 0:300h to 0:3d6h. This overwrites part of the interrupt vector table, but it is a part that doesn't get used very much. This means that these d7h bytes are memory resident without having to use any of the TSR calls of Dos, and without having to reserve part of high memory. Reserving part of high memory is the usual ploy used by Boot Sector Viruses, but the drawback of that route is that you might notice that a few kb from your 640 kb has disappeared (CHKDSK would reveal this). The method used by Twelve Tricks would not show up as a loss from your 640 kb.

When the computer is started up, a random number generator determines which of the Twelve Tricks will be installed. It does the installation by replacing one

of the interrupt vectors with a vector that points to the Twelve Tricks own code, and then chains on to the original code. The twelve tricks are:

1. Insert a random delay loop in the timer tick, so that 18.2 times per second, the computer executes a loop that is randomly between 1 and 65536 long (different each time it is executed). This slows the machine down, and makes it work rather jerkily.
2. Insert an End-Of-Interrupt in the timer tick. This interferes with the servicing of hardware interrupts, so for example, the clock is stopped, TSRs that depend on the timer tick don't work, and the floppy motor is permanently on.
3. Every time a key is pressed or released, the timer tick count is incremented by a random number between 0 and 65535. This has a variety of effects; programs sometimes won't run, when you type "TIME" you get "Current time is divide overflow", and copying files sometimes doesn't work.
4. Every time interrupt 0dh is executed, only do the routine three times out of four. Interrupt 0dh is used on PCs and XTs for the fixed disk, on ATs for the parallel port.
5. Every time interrupt 0eh is executed, only do the routine three times out of four. Interrupt 0eh is used for the floppy disk.
6. Every time interrupt 10h is called (this is the video routine), insert a delay loop that is randomly between 1 and 65536 long (different each time it is executed). This slows the video down, and makes it work rather jerkily and/or slowly.
7. Every time the video routine to scroll up is called, instead of the requested number of lines being scrolled, the entire scrolling window is blanked.
8. Every time a request is made to the diskette handler, it is converted into a write request. This means that the first time you try to read or write to a diskette, whatever happens to be in the buffer will be written to the diskette, and will probably overwrite the boot sector, FAT or directory, as these must be read before anything else can be done. If you try to read a write protected diskette, you get "Write protect error reading drive A". If you do a DIR of a write enabled diskette, you get "General Failure ...", and if you inspect the diskette using a sector editor, you'll find that the boot and FAT have been zeroed or over-written.
9. Every time interrupt 16h is called (read the keyboard) the keyboard flags (Caps lock, Num lock, shift states etc) are set randomly before the keystroke is returned. This means that at the Dos prompt, the keyboard will only work occasionally. Programs that poll interrupt 16h will be unusable. Holding down the Del key will trigger a Ctrl-Alt-Del.
10. Everything that goes to the printer is garbled by xoring it with a byte from the timer tick count.

11. Every letter that is sent to the printer has its case reversed by xoring it with 20h. Also, non-alpha characters are xored, so a space becomes a null, and line feeds don't feed lines.

12. Whenever the Time-Of-Day interrupt (1ah) is executed, do an End-Of-Interrupt instead. This means that you can't set the system clock, and the time is set permanently to one value.

These are the twelve tricks. In addition there are two more things that the trojan does. It uses a random number generator; one time out of 4096, it does a low level format of the track that contains the active boot sector; this will also destroy part of the first copy of the FAT. You can recover from this by creating a new boot sector, and copying the second copy of the FAT back over the first copy. After it does the format, it will display the message "SOFTLoK+ " etc as above, and hang the computer.

If it doesn't do the format, it makes a random change to a random word in one of the first 16 sectors of the FAT, which will make a slight and increasing corruption in the file system. This is perhaps the worst of the things that it does, as it will cause an increasing corruption of the files on the disk.

#### The Dropper program

The program that drops the trojan was, in the specimen that we analysed, a hacked version of CORETEST, a program to benchmark hard disk performance. The file is CORETEST.COM, it is version 2.6, (dated 1986 in the copyright message) had a length of 32469 bytes, and it was timestamped 6-6-86, 9:44. When we looked in more detail at this program, we found some interesting things.

It looks as if the original CORETEST program was an EXE file, and the trojan author prepended his code to it. This code consists of some relocation stuff, then a decryptor, to decrypt the following 246h bytes. The decryption is a double xor with a changing byte. Those 246h bytes, when run, examine the memory to try to find one of five sets of hard disk handler code (presumably corresponding to five Bioses). When it finds one of them, (we have identified the first one as being the IBM XT Bios) it plants the trojan MBR in place, using a far call to the Bios code. The trojan MBR is 200h of the 246h bytes. The trojan is patched so that it also does disk accesses using a far call to the same location. Finally, the prepended trojan passes control to the original program. We call the combination of the prepended code, plus the original program, the Dropper.

The main purpose of the encryption, we would guess, is to evade detection by programs that check code for bombs and trojans. There are no suspicious strings or interrupt calls in the code until it is decrypted at run time.

As far as we can tell, it is not a virus, but a trojan. However, it is unlikely that all the patching to the original program was done by hand - it is far more likely that the trojan author wrote a prepender program (we would call this the Prepender), to automatically attach his code to the target executable. If this is the case, then there are two consequences. The first is that he might have trojanised other programs besides the one that we have examined. In other words, there might be other Droppers around besides the one we have examined. The second is that if that is the case, we cannot rely on the

encryption having the same seed each time, as the Prependers might change the seed each time it operates. So it would be unsafe to search files for the encrypted MBR. Instead, we propose a search string based on the decryptor.

Indeed, a further possibility exists. The Prependers program might have been placed into circulation, and people running it would unwittingly be creating additional Droppers. There is absolutely no evidence to suggest that that is actually the case, but we would ask anyone who detects this Dropper in one of their files, to also examine all the others.

#### Detection

Here's a variety of ways to detect the trojan. The hexadecimal string e4 61 8a e0 0c 80 e6 61 is to be found in the MBR. This string will also be found in memory if you have booted from a trojanised MBR, at location 0:38b. You can use Debug to search in memory.

A useful search string to detect the Dropper is

```
be 64 02 31 94 42 01 d1 c2 4e 79 f7
```

#### Getting rid of it

It's easy to get rid of Droppers; just delete them and replace them with a clean copy. If you find the string above in the MBR or in memory at 0:38b, you need to boot from a clean Dos diskette and replace the partition record. DO NOT use Fdisk to do this unless you are prepared for Fdisk to zero your FAT and directory; you will lose all your data that way. One way would be to do a file-by-file backup, low-level format to get rid of the trojan MBR, then Fdisk Format and restore your backup. We would recommend doing two backups using as different methods as possible if you use this route, in case one of them fails to restore.

The other way to replace the partition is to run a program that drops a clean partition record onto the MBR, but doesn't change the partitioning data. We are currently preparing one of these - please ask if you need it.

#### Damage done

The whole of the MBR is used for the code. Most normal MBRs don't use more than half the space, and a number of other programs have started using this space. For example Disk Manager, and the Western Digital WDXT-Gen controllers (but the Dropper doesn't work on the WDXT-Gen). This means that the Dropper might cause an immediate problem in some circumstances.

The main damage done, however, will be in the impression that this trojan creates that your hardware is suffering from a variety of faults, which usually go away when you reboot (only to be replaced by other faults). Also, the FAT gets progressively corrupted.

#### Occurrences

So far, this has only been reported in Surrey, England. It was noticed because

it made a disk using Speedstor to control it, non-bootable. Disks that are controlled in the normal way, remain bootable. We would be grateful if any sightings could be reported to us, especially if the Dropper program is different from the one we have examined; we would also like a specimen of it,

Please report instances to the addresses below:

Dr Alan Solomon            Day voice: +44 494 791900  
S&S Anti Virus Group      Eve voice: +44 494 724201  
Water Meadow              Fax: +44 494 791602  
Germain Street,            BBS: +44 494 724946  
Chesham,                    Fido node: 254/29  
Bucks, HP5 1LP            Usenet: drsolly at ibmpcug.co.uk  
England                    Gold: 83:JNL246  
CIX, CONNECT drsolly

or

Mr Christoph Fischer      Day voice: +49 721 6084041  
Micro-BIT Virus Centre    Eve voice: +49 721 861540  
University of Karlsruhe    Fax: +49 721 621479  
Zirkel 2                    BITNET: RY15 at DKAUNI11  
D-7500 Karlsruhe 1  
West-Germany



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 9: Issue 71

Monday 26 February 1990

## Contents

- [Journalists and computers: `Z'](#)  
[R. Clayton](#)
- [Space Shuttle](#)  
[Steve Bellovin](#)
- [Magellan spacecraft will need frequent guidance from Earth](#)  
[David B. Benson](#)
- [More on Air India Airbus A320](#)  
[Steve Milunovic](#)
- [AT&T](#)  
[Clifford Johnson](#)  
[Rob Warnock](#)  
[Steve Bellovin](#)  
[David Paul Hoyt](#)
- [Re: Computerized Collect Calls \(John J.G.\) Mainwaring](#)
- [A different multiple-copy problem \(SEN\)](#)  
[Dan Craigen](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✉ Journalists and computers: `Z'

*R. Clayton <clayton@thumper.bellcore.com>*

*Wed, 21 Feb 90 15:04:48 EST*

Earlier this year, the New York Times published an anonymous op-ed piece about Gorbachev's reforms. Since the piece was quite pessimistic, speculation arose about the author's identity. The 19 February 1990 issue of The New Republic has an article by Lionel Barber identifying the author as historian Martin Malia at U. C. Berkeley. Among the reasons given for this choice was:

The hardest evidence, however, comes from Berkeley's own history department. According to a staff member whom I interviewed, Malia composed part of the Daedalus article [a longer version of the op-ed piece] on a departmental computer under the filename "PERES" -

presumably a reference to perestroika, not the Israeli politician. The staff member called up the file on his own computer during our interview and read me lengthy passages, all of which were identical to passages in "To the Stalin Mausoleum" [the title of the Daedalus article].

A few pages further on in the same issue, Katie Hafner (who I believe was causing a stir elsewhere on the network recently) has an article on the Robert Morris trial. Her conclusion was that Morris' conviction was a small step for some abstract principle, but had little or no relevance to practical concerns about computer crime.

---

## **✶ Space Shuttle**

<smb@ulysses.att.com>  
Sun, 25 Feb 90 19:57:36 EST

Sunday's launch of the space shuttle was delayed because of problems with the backup tracking computer used by the range safety officer. According to the Air Force, the problem was "bad software". No word, at least in the stories I've seen, about what the bug was, or about why it affected only the backup computer -- or how long this bug has been present.

--Steve Bellovin

---

## **✶ Magellan spacecraft will need frequent guidance from Earth**

David B. Benson <dbenson@cs2.cs.WSU.EDU>  
Wed, 21 Feb 90 11:51:36 PST

Idahonian/The Daily News, Weekend, February 17 & 18, 1990

PASADENA, Calif. (AP) -- The Magellan spacecraft speeding toward cloud-shrouded Venus on a \$550 million mapping expedition, will need frequent commands from Earth until NASA fixes a computer problem.

Despite the failure of a computer chip on the spaceship, "there's no threat to the mission," said Edwin Sherry, a technical assistant at the space agency's Jet Propulsion Laboratory.

Until engineers locate the faulty chip, they must send Magellan new commands every other day to make sure it is pointing in the proper direction, Sherry said.

He said a similar computer chip failure happened before Magellan was launched and that such a failure is expected about once annually. "You'd hope for zero faults like this," Sherry said. "But they're typical of working with state-of-the-art equipment. It's remarkable we have so few."

Magellan was launched from space shuttle Atlantis on May 4. It will go into a polar orbit around Venus on Aug. 10.

[Two paragraphs about the mission deleted.]

The problem developed Sunday as the spacecraft got ready to take a fix on two distant stars to make sure it was pointing the right way. An

error was detected in a tiny part of Magellan's computer memory.

The error prompted Magellan to shift to a backup computer and point its solar panels toward the sun to increase the power supply.

The failure was apparently the result of electrical corrosion at a junction between two types of material on a single memory chip, leaving the chip unable to remember anything, Sherry said.

He said, however, engineers haven't yet ruled out the possibility that the chip was damaged by an electrically charged particle spewed out by the sun, which is near the peak of its 11-year cycle of activity.

Magellan uses gyroscopes to sense when pressure from solar wind makes the spacecraft drift slightly, or point in the wrong direction. The gyroscopes normally issue automatic commands to three spinning wheels, which correct the spacecraft's alignment.

Magellan's main computer is programmed to take a fix on the two stars each day to determine the spacecraft's actual alignment. If this "star calibration" shows the gyroscopes failed to align Magellan correctly, they again command the wheels to adjust the craft's position.

[Oh well, its only an AP staff reporter...]

[I recall that there is also some computer problem with Galileo, maybe from an article in AAAS Science, but I haven't seen it on RISKS.]

---

### ✂ More on Air India Airbus A320

Steve Milunovic <Steve\_Milunovic@quikmail.sri.com>

Mon, 26 Feb 1990 13:23:04 PST

Crash in India Rekindles Dispute over Safety of Airbus A320 Jet  
(Steven Greenhouse, c.1990 N.Y. Times News Service, BRIEF EXCERPT)

PARIS. The crash of an Airbus A320 jet that killed 97 people in India last week has reignited a dispute in France over whether the computerized, highly advanced aircraft is too complicated to fly. The French pilots union is urging the airliner be grounded in France. "This plane is sometimes put into operation by people who aren't qualified enough," said Jean-Claude Bidot, secretary general of the French Airline Pilots Union. "It's a supercomplicated aircraft."

But the maker of the plane, the four-nation consortium known as Airbus Industrie, said the plane was quite safe and the French pilots were opposing it to protect their economic interests. The plane uses two pilots; many other aircraft use three. [...]

---

### ✂ AT&T (Kamens, [RISKS-9.69](#))

"Clifford Johnson" <GA.CJJ@Forsythe.Stanford.EDU>

Fri, 23 Feb 90 16:15:41 PST

> "do . . . while" construct, which contained a "switch" statement, which

This presumes that the error was made by one particular programmer. But such production code is surely the responsibility of a team of programmers, each

module being evaluated by more than one peer and supervisor. All programmers make errors. The problem is why this "stupid programming error" survived through to production. Correcting the code does not correct this root problem; and the root problem, failure to catch the error, may be less likely in other languages.

> if we can't expect our programmers to understand the language  
> with which they are programming, then what \*can\* we expect?

Certainly, we must expect programmers to make such mistakes whatever their language, and however well they understand it. Some languages do assist error-catching more than others, APL being the extreme worst case, for example.

### **✂ Re: Problems/risks due to programming language, ... ([RISKS-9.69](#),.70)**

*Rob Warnock <rpw3%rigden.wpd@sgi.com>  
Fri, 23 Feb 90 22:35:06 PST*

The BLISS family of languages originally had this hazardous multi-level break, "EXIT[n]", but then they added (\*sigh\*) a better scheme. Any expression (and in BLISS, \*all\* control structures such as begin/end, if/then, case, for/while loops, etc, were expressions and could yield values) could have a label attached, and from anywhere within that expression only you could say, "LEAVE <label>" or "LEAVE <label> WITH <value>". That way, the thing being left stayed constant even if you added or removed interior levels. Further, labels had to be declared before being used (generally considered a pain, until the day it saved you from a misspelling), and a label could be used -- attached to something -- only once in the scope of its declaration. (Of course, you could have many LEAVE's inside a labelled structure.) Outline:

```
LABEL FOO;
LOCAL X;
```

### **✂ C problems?**

*<smb@ulysses.att.com>  
Sat, 24 Feb 90 02:01:52 EST*

There is little point to enumerating the vulnerabilities of C; one could write a book about them. In fact, Andy Koenig already has: "C Traps and Pitfalls", which I recommend to anyone using the language. That is not the point, however. The real question is whether or not any real language is sufficiently free of such traps as to significantly reduce the probability of errors.

To tremendously oversimplify the situation, languages that are higher-level than C often achieve their power at the price of complexity. This complexity itself can breed errors; see, for example, Hoare's comments on Ada, or Koenig's early paper "PL/I Traps and Pitfalls". To be sure, the power can help avoid some bugs -- the "fingerd" bug that the Internet virus/worm/parasite exploited could not have happened in PL/I because strings, and in particular variable-length strings, are a built-in data type; one would

not have C's temptation to use fixed-size arrays.

On the other hand, languages that are "safer" than C often achieve their safety by significantly restricting their expressive power. This can have several results. First, the programmer must concentrate more on low-level details again, with the concomitant pressure towards short cuts (i.e., fixed length arrays -- Pascal, for example, does not even have malloc()). Second, the language may become unsuitable for large projects; again, Pascal comes to mind. Third, programmers will cheat -- move around the boundaries of the language using escape hatches or arcane knowledge.

It may be that there is a suitable compromise. There have certainly been enough attempts; what is missing is convincing evidence that these actually reduce the error rate in real life. Note that by "real life", I specifically include the lifetime history of real programs -- and that includes modifications and changes over the years by many different people. I assume that there have been some attempts to measure this; I would appreciate citations.

The other approach often taken is to design languages that are in some sense "suitable for verification". That is, features are inserted or omitted not simply because of their complexity or aesthetics, but also because of their effect on attempts to verify the program using formal methods. Apart from the aforementioned question of whether or not such languages are really suitable for real programming problems, they do nothing in and of themselves to reduce the error rate; they merely make it easier for a competent, well-trained programmer with enough time to validate a program as its being written. (Some would claim that writing a program using formal methods will result in less-buggy programs. I will not dispute that here, except to note that that requires more time up front -- and we all know how feasible that can be when on a tight schedule, even if it seems likely to reduce total project time later on.)

If such languages help, though, we are very far from our original ideal, which was a technical solution to the problem. Verifying programs, or constructing them using formal methods, requires rather different, and arguably scarcer, skills than are present in the programming population today. It is thus a people problem, and an educational one. In fact, it is far from clear that this will accomplish very much overall except to recast the obvious: that better programmers write better programs. Wasn't it Knuth who demonstrated years ago that the best programmers produced code that was 4-5x faster \*and\* 4-5x smaller than the worst?

Our goal must be to let anyone write better programs. The challenge is not only devising the methods, but also demonstrating that they work.

--Steve Bellovin

---

**RE: AT&T (Smith, [RISKS-9.70](#))**

*david paul hoyt <YZE6041@vx.acs.umn.edu>  
Sat, 24 Feb 90 12:24 CST*

> If the AT&T programmer had coded "goto" instead of "break", ...

The reason the programmer would have had problems with his/her peers is that (unconstrained) goto's greatly reduce the maintainability of the code.

Ultimately increasing the likelihood of failure. In my experience, it has been very rare that with a little more thought, I couldn't come up with a solution that got rid of the need of a goto. Non-local goto's are almost always a sign of unwarranted complexity and that the design should be rethought. By the way, I am experienced in large scale complexity. I have developed, maintained and converted +million line programs.

david | dhoyt@vx.acs.umn.edu | dhoyt@umnacvx.bitnet

---

### ✂ re: Computerized Collect Calls

*John (J.G.) Mainwaring <CRM312A@BNR.CA>*

*Fri, 23 Feb 90 16:20:00 EST*

Mark Brader's posting in [RISKS-9.69](#) about the reporter who reached the editor who said "... computer telemarketing things" just goes to illustrate one of the pervasive threads of this forum: Computer Aided Stupidity will have far more impact on society than Computer Aided Intelligence for years to come. Mark's reporter and editor seem to be cases in point.

Automated systems such as this have easy mechanisms to allow the user to talk to a live operator when the automated system doesn't meet their needs. It does have to occur to one or other of the users (in this case the reporter) that the live operator would be a good idea. Automation is brought about because of consumer pressure brought on the PUCs which control the telephone operating companies' rates. If you would really prefer an all manual system, perhaps next time your PUC is considering a rate application from your telephone company, you will go along and tell them you don't think the phone company is asking for enough. By and large, this is an uncommon occurrence.

Perhaps we could all entertain ourselves with stories about how when you call with these new fangled rotary dial phones, they don't even know that Millie is always next door at Dottie's having coffee at this time of the morning like the operator always knew. I doubt if there ever was or will be an innovation involving something we all use every day that doesn't let someone come up with a story to convince himself he's (marginally) smarter than some machine. Once the new becomes familiar we usually really do end up in control of the machines.

---

### ✂ A different multiple-copy problem (SEN)

*Dan Craigen <dan@ora.on.ca>*

*Sat, 24 Feb 90 00:19:57 EST*

Unfortunately, we're all used to receiving multiple copies of the Risks digest from time to time. However, when I got home today, I found twelve copies of

Software Engineering Notes at my front door. Apparently, somewhere along the distribution line, the twelve copies were bundled together with my name and address at the top. The other eleven are for various individuals spread out through Ontario. The ordering of the journals is based on ACM membership number.

An interesting Risks twist. I'll put the other eleven back in the postal system tomorrow.



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 9: Issue 72

Wednesday 28 February 1990

## Contents

- [Clients cross about crossed wires](#)  
[David Sherman](#)
- [100-year-old can drive four years without test](#)  
[David Sherman](#)
- [Some comments on the Airbus](#)  
[Robert Dorsett](#)  
[Martyn Thomas](#)
- [Re: Problems/risks due to programming language](#)  
[Bruce Hamilton](#)
- [Comments on programmer error](#)  
[Geoffrey Welsh](#)
- ["Goto considered harmful" considered harmful](#)  
[Brad Templeton](#)
- [lockd](#)  
[Caveh Jalali](#)
- [Re: Railroad interlocking systems](#)  
[J.A.Hunter via Brian Randell](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✂ Clients cross about crossed wires

*David Sherman <dave@lsuc.on.ca>*

*Mon, 26 Feb 90 16:47:29 EST*

Toronto Star, February 25, 1990:

BROCKVILLE (CP) - Ma Bell got a wrong number last month -- 17,000 times. That is the number of long-distance calls incorrectly charged to telephone numbers in Iroquois, Ont. A Bell Canada official has described the mistake, blamed on computer error, as the company's biggest foul-up in years.

During the billing period from Jan. 12 to Feb. 16, calls made by residents of Athens, Ont. were charged to customers in the Iroquois exchange. [...] I've never seen anything like this in my seven years as area manager," said Ron

Kristiansen, customer services manager for Bell's Brockville, Kingston and Belleville exchange areas. Some Iroquois customers reports they had been charged for up to 40 long-distance calls they had not made, more than doubling their monthly phone bills.

---

### **✂ 100-year-old can drive four years without test**

David Sherman <dave@lsuc.on.ca>

Mon, 26 Feb 90 07:55:31 EST

Toronto Star, February 26, 1990:

"I think it's stupid -- the whole damn thing," grumbled Charles Narraway. The Nepean, Ont. [suburb of Ottawa - DS] resident will be 100 years old in March, and that seems to have turned up a bug in the transportation ministry's computer. For 20 years, Narraway has had to take an annual road test o get his driver's license renewed. And for 20 years he passed it the first time, every time. But this year he got a license, good for four years, without a test. Narraway's driver's license shows his date of birth as 90-03-04, and he figures the computers have tacked the wrong century on to the front...

[Some of you will recall the story of the man whose insurance rates tripled (high-risk) when he turned 101. The computer truncated... PGN]

---

### **✂ Some comments on the Airbus**

Robert Dorsett <rd@walt.cc.utexas.edu>

Mon, 26 Feb 90 23:28:54 -0600

Dave Morton wrote in [RISKS-9.65](#):

> We talked about the  
> Airbus crash and it seems that in pilot circles it was attributed to the  
> fact that the older Airbus machines had Rolls-Royce engines. It seems that  
> when given full power they reacted about 3 seconds faster that those on  
> The A320. In his opinion these three seconds were vital.

However, it's a totally different category of engine (CFM-56 vs. large-fan). Different airplanes require different approaches, and "type conversion" training is usually very thorough. The pilots in question also had 300-odd hours in type (each), 10,000+ hours of experience (each, distributed among different aircraft types), and the captain (who was flying) was the chief of A320 training for Air France. What's noteworthy about the Mulhouse-Habsheim crash was the lack of formal cockpit procedures and the lack of flight crew experience in the type of maneuver performed. It was almost definitely pilot error.

>a role in his judgement. On a side note the pilot also mentioned that the  
>757, which also has the fly by wire system, sometimes "hangs". The only  
>way to get the electronics to function again is to power cycle the lot.

That may be so, but it's not possible to extend the lesson to the A320, since the design of the systems are totally different (the fundamental \*design\* philosophy as regards pilot access to the electrical system is different, too). And as a small note, the flight augmentation system of the 757 is in no way comparable to the A320's fly-by-wire system (or its associated software protections). The former is dedicated to damping aerodynamic instability; the former introduces new \*control laws\* and appears to be intended to work around problems involved in the use of side-stick controllers.

George Michaelson wrote in [RISKS-9.69](#):

>I find it hard to raise any possible risks in technology transfer to developing  
>countries (does that label apply to India?) given the overtones of chauvinism  
>if not downright racism

This sentiment bugged me--light-footing it around safety-critical issues because they might reflect poorly of the policies of developing nations. Bugged me enough to write a rather long-winded response (which I'll be glad to email to anyone who's interested in my ramblings). Suffice it to say that maintenance \*is\* a critical issue among all airlines operating new equipment, and that the situation is \*particularly\* serious in developing nations.

Udo Voges wrote in [RISKS-9.70](#):

>have decided to require an extended basic training in India. The pilot S. S.  
>Gopujkar was probably acting as an instructor during the accident flight on  
>last Wednesday (14 Feb 90 uv), despite the fact that he didn't have the  
>required qualification. This would explain, why he asked the control tower to  
>make a manual landing on sight.

The problems in this account are:

1. No airline that I'm aware of performs simulated in-flight systems failures on revenue flights.
2. Airbus proper regards "manual" (electric horizontal stabilizer trim and manual rudder) backup as a last-ditch emergency system. Numerous reports indicate that its operation isn't even part of the standard Airbus training curriculum. It's not something that a marginal pilot is likely to be playing with. Marginal pilots tend to hide \*within\* automation, to become systems managers, rather than pilots.
3. It's highly unusual for an aircraft to consult with an air traffic control facility on the operation of an on-board system (unless, of course, the pilot expected to crash).

The account sounds highly suspect. Upon examination, various terms could be examined--perhaps "manual" means hand-flying it (with protections) to the ground, rather than tracking an ILS, and the tower wished to confirm that the ILS wouldn't be used or something. I don't know. But note that if this IS the case, the A320's "safety" features should prevent precisely this sort of crash--the pilot should be able to fly to the surface, jerk back on the stick, do the most violent maneuvers, etc--all without crashing the airplane (that is, above 100', beneath which the protections disappear).

> So again it is - only - human malfunctioning (insufficient training,  
> bad management procedures, financial reasons ?). Udo Voges

But then the question is: assuming that the systems ARE working properly, when does it stop being "human error" and become poor ergonomics? RISKS has traditionally concentrated on software or hardware reliability issues, which are in themselves important issues. But don't forget that the very way the pilot INTERACTS with the aircraft is also a safety issue, and the A320 has thrown the lessons painfully learned over the past 80 years right out the window.

Indeed, on a more general scale, the A320 is only the most extreme example of a disturbing trend. If one studies the different cockpit designs of airplanes introduced since 1981 (all of which use different display formats on CRT-based flight and engine instrumentation), one starts to recall the absolute lack of standardization that was rampant during the 1920's, 30's, and 40's. When one considers the problems this will cause in training, and factors in pilot gullibility (perhaps believing what the manufacturer says about the safety features of the airplane--I find it quite amusing that the pilot opponents to excessive automation or fly-by-wire are being branded with '50's-mentality "anti-progress" labels), I suggest that we can probably expect the same sort of safety records.

---

### **✂ A320 sidesticks**

*Martyn Thomas <mct@praxis.UUCP>  
Tue, 27 Feb 90 16:51:23 BST*

The A320 sidestick layout is asymmetric - the captain flies with the left hand, the first officer with the right. This means that when the first officer is flying in the left-hand seat - as will happen from time-to-time, e.g., for training - there is the added unfamiliarity of using the other hand.

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK.

[It is pessimal when the captain is right-handed and the first officer is left-handed and *\*both\** are flying with the *\*wrong\** hand. But the switching back and forth must undoubtedly be confusing. PGN]

---

### **✂ Re: Problems/risks due to programming language**

*Bruce Hamilton <BHamilton.osbuSouth@Xerox.COM>  
26 Feb 90 17:48:40 PST (Monday)*

I'm incredulous at the number of replies seeming to say, "No language prohibits all errors, so we might as well use "C".

Some 25 years ago, PL/I had named scopes. You can say something like

Foo: BEGIN

```
...  
EXIT Foo;  
...  
END Foo;
```

and the EXIT has a clearly-defined scope, irrespective of how many intermediate levels of nesting there are.

--Bruce 213/333-8075

---

### **✂ Comments on programmer error by Clifford Johnson & others**

*Wed, 28 Feb 90 11:46:17 EST*

In [RISKS 9.71](#), there seems to be a general discussion of programmer error and its inevitability. I think that the entire discussion can be summarized as follows (sorry, I don't know who originally wrote this):

The tendency to err which programmers have been noticed to share with other human beings has often been treated as if it were an awkwardness attendant upon programming's adolescence, which (like acne) would disappear with the craft's coming of age. It has proved otherwise.

For years I avoided `C' because I was literally intimidated by the ease with which one can confuse oneself, such as:

```
#define square(x) ( x * x )  
[...]  
b = square( a++ );
```

Eventually a wise friend pointed out that no language can hope to second-guess your intentions and point out possible errors in logic, and that few programmers could maintain their sanity near a compiler that did so. Since then I've developed a few rules of thumb, such as not modifying the contents of more than one variable per line wherever possible (a natural outgrowth of having done some assembler), and I have been able to put out occasional `C' code that is neither more nor less buggy on average than what I write in any other language - though that doesn't say much!

Geoff Welsh, 602-66 Mooregate Crescent, Kitchener, Ontario N2M 5E6 CANADA

---

### **✂ "Goto considered harmful" considered harmful**

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

*Wed, 28 Feb 90 14:42:03 EST*

This is a most unusual RISK. That famous paper put the poor GOTO so out of vogue that programmers are actually afraid of using it -- they will make their programs more complex and harder to understand in order to avoid using the dreaded goto.

They do this out of fear of rejection. Some great programmer will read their code, see the "goto" and go tsk-tsk. Horrors.

Because C has no multi level break or continue, the use of a goto to do loop exception handling detracts in no way from the "structuredness" of the program.

But the fear of the stigma of goto has lead programmers to bugs, it seems. Yet another example of a RISK due to fear of RISKS.

Brad Templeton, ClariNet Communications Corp. -- Waterloo, Ontario 519/884-7473

---

## **lockd**

*Caveh Jalali <caveh@csl.sri.com>*

*Mon, 26 Feb 90 13:34:05 -0800*

To lock is to block! sometimes.

Due to a bug in SunOS 4.0.3, lockd (/usr/etc/rpc.lockd) will occasionally dump core on NFS servers. This happens silently and goes unnoticed until some NFS client attempts to lock a file on that server.

As a result, a process requesting a file lock on a file will block on disk wait indefinitely ('D' state report from ps) until lockd is restarted (manually) on the NFS server for that file.

The quickest way to detect this is to check for a core file in /. "file /core" will provide the name of the process which is responsible for the core file. Now, quickly check if that process is still around using "ps". If it is not, it is probably necessary to restart the service manually. In the case of lockd, it is sufficient to:

```
cd / ; /usr/etc/rpc.lockd
```

to restart/restore the service. The "cd" makes sure the next core dump will go in / again, which is where we "expect" it.

00c - Caveh Jalali

[Our MM -- but not RISKS' --was out of commission as a result of the lockd problem. The LOCK-MESS MONSTER STRIKES AGAIN. BY THE WAY, we are backing off to a 'less advanced' (old standard) SENDMAIL. It will probably be ready for the next issue of RISKS, so please stand by for a different set of horror tales. We had a dilly yesterday when SENDMAIL suddenly started spawning processes like crazy, and had to be killed. PGN]

---

## **Re: Railroad interlocking systems**

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

*Tue, 16 Jan 90 11:44:35 BST*

A short while ago I passed a message I'd seen on the net (in RISKS?) about railway interlocking to one of my colleagues here at Newcastle who is very interested in such topics. He gave me permission to forward his reply to RISKS, so here it is.

Brian Randell

=====

>From: J.A.Hunter@newcastle.ac.uk

With reference to:

> Date: Fri, 5 Jan 90 09:49:21 CST

> From: Douglas W. Jones <jones@pyrite.cs.uiowa.edu>

> Subject: Railroad interlocking systems

> [...]

> I suspect that there are useful parallels between the history of railroad  
> interlocking machines and the more recent developments in safety critical  
> digital control systems. An error in the logical design of an interlocking  
> machine could easily go undetected until it caused a train wreck, and I  
> wonder if old cases involving railroad interlocking machines might provide  
> useful precedents for many of the software liability questions that have been  
> raised recently.

There's one case in British railroad history of an interlocking frame being in service for many years and then (apparently) causing a train wreck. It happened on February 14th, 1928 at Paragon Street station, Hull, in the East Riding of Yorkshire.

The area had a large and complex track layout controlling several main and secondary lines and freight routes to the local dockyards. On that day two trains met head on, one having been incorrectly routed onto the wrong track. The signal box (control tower) in question would have had around two hundred levers and had three signalmen in charge.

To understand the accident it is necessary to realise that signalling safety depends on more than just the interlocking frame. There are trackside devices that "prove" the position of points and signals and prevent, for instance, a signal being cleared if the switch it refers to has not been set appropriately, with both blades in position and locked. Additional equipment detects the presence of a train to prevent a switch being moved under it. These days this is done using electrical track circuits, in which the presence of a train is detected by the short-circuit through the axles from one rail to the other, but in mechanical systems this was not always present and various mechanical detectors were used. One of these was a treadle fitted near to switches; depressed by the flanges of the vehicles' wheels, it locked the switch in place until cleared.

In the Hull accident, the signalmen were concerned not to delay a late running train and one of them reset the signal cleared for train A after the locomotive and three coaches had passed it. At this point the locomotive was still thirty feet from the trackside treadle which would lock the next switch during passage. During the time the train took to reach the treadle, less than a second, it had effectively disappeared from the logic of the interlocking





Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 9: Issue 73

Tuesday 6 March 1990

## Contents

- [Another 100-year computer saga](#)  
[David B. Benson](#)
- [Traffic System Failure](#)  
[Rich Neitzel](#)
- [Railway interlocking systems](#)  
[Clive Feather](#)
- [Avionics in the media](#)  
[John M. Sullivan](#)
- [Re: A320](#)  
[Steven Philipson](#)  
[Subhasish Mazumdar](#)  
[Pete Mellor](#)
- [Mileage Plus wants me to move](#)  
[Tim Kay](#)
- [Credit-card fraud](#)  
[Douglas Mason](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✉ Another 100-year computer saga

*David B. Benson* <[dbenson@cs2.cs.WSU.EDU](mailto:dbenson@cs2.cs.WSU.EDU)>  
*Sun, 4 Mar 90 14:13:34 PST*

Chemical & Engineering News, February 26, 1990, p. 168:

Physician Beatrice Golomb tells of a 99-year-old man who turned up in the emergency room (JAMA, Dec. 8, 1989, page 3132). His white blood cell count, although far out of line, was reported by the computer to be within normal limits. The computer, it turned out, was reporting values for the newborn, having figured that year of birth, plugged in as '89, was 1989, not 1889. Golomb's comment: "The normal ranges provided by hospital computers are not always to be credited."

[And what with happen to the 102-year-old admitted on 2000 Jan 01?]

---

## **✂ Traffic System Failure**

*Rich Neitzel <thor@stout.UCAR.EDU>*

*1 Mar 90 14:13:47 GMT*

On Tuesday Feb. 27, 1990, the central computer that controls the traffic light timing for the city of Lakewood (a major suburb of Denver) failed, causing traffic delays of over 30 minutes. The computer system's disk drive suffered a burnt and seized bearing, causing it shut itself down.

The replacement of the drive did not occur until the next evening.

Several interesting items related to this incident:

1> The system has exactly one drive. No redundancy (sp?). Of course, they do backup the disk, however, since there is only one disk drive, they had nowhere to put the backed data. (The disk crash apparently eat the disk media). From past experience with supposedly critical computer systems, it would seem that this is common. Concern about reliability of computer systems to most operators of said systems seems to stop once they are assured that no data will be lost. Of course, it never seems to occur to them that if they cannot access that data it's useless.

2> All of Lakewood's traffic system is controlled by one computer. Need I say more?

3> The traffic system was apparently design under the impression that a computer failure would be virtually impossible. When the computer failed, traffic lights had no fall back mechanism for running under a reasonable cycle time. Each light had to be manually set by city traffic crews.

One wonders if this kind of traffic control system is representative of common practice. If so, think - you could immobilize a major urban area by knocking out three or four computer systems.

Richard Neitzel, National Center For Atmospheric Research  
Box 3000 Boulder, CO 80307-3000      303-497-2057

---

## **✂ Railway interlocking systems**

*Clive Feather <clive@ixi.UUCP>*

*Fri, 2 Mar 90 12:46:37 gmt*

[Quoting J.A.Hunter via Brian Randell]

> Modern British practice requires that once a route has been set, a time delay  
> of about one minute is enforced by the software before a conflicting route  
> can be set.

The actual practice is that if the signal governing entry to the route is at "Danger", the route can be cancelled immediately (by pulling the button for that route on the panel). If the signal is in any other state (i.e. a train could legally pass it), then the route is locked for a while. Simple locking locks the route for 2 minutes (not 1). Comprehensive locking only locks the

route if there is a train near enough to the signal to be affected by it turning red, and waits until that train has come to a stop at the signal (e.g. has occupied a 200m track circuit at the signal for 30 seconds). If a train passes a signal at Danger, points ahead of that signal are locked automatically.

> That such systems are not perfect and still rely on human vigilance was shown  
> by the Clapham (South London) accident late in 1988 where a faulty track  
> circuit train detector "lost" a train standing at a signal allowing an  
> automatic system to route another train into the rear of it.

This accident was caused by faulty installation. At the time, the signalling system was being replaced by a new one, and a wire had been removed from the logic concerned with a certain track circuit. The wire had not been cut back and had its end insulated, but was just bent out of the way. Later work on that logic disturbed the wire, and it came back into contact with the terminal it had been removed from. It then fed current into the logic, making it appear as if the track was clear. This allowed the signal to turn green.

> A good source book for information on British railroad safety is:

>  
> "Red for Danger", by L.T.C.Rolt,  
> published by David & Charles Inc. (North Pomfret, Vermont 05053),  
> ISBN 0-7153-8362-0

Not just a good book, but the definitive one. The current edition has been updated by Geoffrey Kitchenside.

BTW, it's railway.

^^^

Clive D.W. Feather, IXI Limited, 62-74 Burleigh Street, Cambridge U.K.

---

**✉ Re: A320 ([RISKS-9.72](#))**

*Steven Philipson <stevenp@decpa.pa.dec.com>*

*Wed, 28 Feb 90 17:19:04 PST*

In [RISKS DIGEST 9.72](#) Martyn Thomas <mct@praxis.UUCP> writes:

>The A320 sidestick layout is asymmetric - the captain flies with the  
>left hand, the first officer with the right. This means that when the  
>first officer is flying in the left-hand seat - as will happen from  
>time-to-time, e.g., for training - there is the added unfamiliarity of  
>using the other hand.

and Peter Neumann writes:

> [It is pessimal when the captain is right-handed and the first officer  
> is left-handed and \*both\* are flying with the \*wrong\* hand. But the  
> switching back and forth must undoubtably be confusing. PGN]

This is not a new risk. Older generation aircraft that have yolks instead of sidesticks are flown in exactly the same manner. Throttles are usually

located in the center panel, and both pilots use their inboard hand for throttles, and their outboard hand to manipulate the yoke. Sidestick controllers just change the position of the hand, but not which hand is used. There are other differences in the use of sidesticks (such as lack of interconnection on the Airbus), but in handedness they are similar to conventional controls.

Switching hands with which one flies is generally viewed as a non-problem. Pilots get used to switching seats and the hands they fly with early on in their training, usually well before they step into a jet airliner cockpit. On a frequent basis I switch between right and left seats and between aircraft yokes (which are flown with the left hand from the left seat) and sticks (which are flown with the right hand from the left seat. The process is natural and not at all confusing.

I have not seen any reports that indicate that there is a significant problem in switching, although that doesn't prove that there is no loss of performance. Pilots reports of difficulty with this are rare (at least, in my experience).

It is far more difficult to change between aircraft types, or even between individual aircraft of the same type, when the positions of instruments and secondary controls vary. Problems arising from such differences are well documented and have been identified as causal in numerous accidents.

---

## **avionics in the media**

*John M. Sullivan <sullivan@math.Princeton.EDU>  
Sat, 3 Mar 90 17:32:25 -0500*

The New York Times has recently had two articles on avionics. On Feb 14, the Business Technology column featured "McDonnell's Less Costly New Jet", the MD-11, which is 16% cheaper to fly than the DC-10, and is intended to "fill a niche" between Boeing's 767 and 747.

The plane contains an automated cockpit that the company calls the world's most advanced, as well as more fuel-efficient engines, some lighter-weight parts and aerodynamic refinements like a shortened tail.

But, later we find that

The plane is a prime example of how aircraft manufacturers are hesitant to introduce new technology if it does not translate into savings for the airlines. "High technology isn't necessarily what an airline wants," said Dale Warren, a vice president at Douglas. "They're in business to make a profit." For example, the company replaced only a few aluminum parts with lightweight composite materials, which are more expensive, and chose not to use a "fly by wire" electronic control system, in part because of its cost.

A few paragraphs describe the cockpit:

The most dramatic change to the DC-10 is in its cockpit, which Douglas says

is the world's most automated. The plane will have two pilots, compared with three in the DC-10; the flight engineer has been replaced by computers that automatically perform duties like monitoring fuel flow and adjusting cabin pressure.

The computers can, to some extent, "think" for the pilots, switching valves if something should go wrong. Pilots watch six video displays run by computers instead of the dozens of mechanical gauges and dials on the DC-10. "Essentially, the pilot pushes a button at the end of the runway and the system will guide the plane to the concrete at the destination," said George Wallace, program manager for Honeywell Inc., which makes the cockpit electronics for the plane.

While similar automated cockpits--already in place on Boeing aircraft and Douglas's MD-80 plane--have won praise, pilots have also expressed concern that their basic flying skills may atrophy.

Douglas chose to use a conventional control system, in which the controls are operated from the cockpit by mechanical means rather than electronically by computers in a new system as "fly by wire" that is used on some Airbus jets.

The article ends by noting that flight testing is 6 months behind schedule.

The Sunday Business section on Feb 18th had a long article "All About: Avionics". This mentioned that "Cockpit electronics have become sophisticated enough to all but take the place of the pilot. ... With the push of a few buttons, autopilots can guide a plane from NY to LA while the real pilot sits back."

The electronics may cost \$1M, or 10% of the plane's price. The article notes that American companies (Bendix/King, Collins Avionics, and Honeywell) dominate the market. Other companies would have a hard time entering the market because of the need for government approval of the systems.

Some problems are discussed:

The biggest advantage of the glass cockpit is that the black boxes can talk to one another. The on-board computers can calculate an altitude for the greatest fuel efficiency and the autopilot can guide the plane there.

Most pilots like the new technology, with some reservations. If something goes wrong, the problem may be hard to detect. "Trouble-shooting is a more delicate art than before," said Wolfgang Demisch, an analyst with UBS Securities. And a three-year NASA study of 200 Boeing 757 pilots found that they were concerned about spending too much time staring at computer screens and not enough looking out the windows. They also worried that their basic flying skills would atrophy as they spent more time punching keypads. "I was somewhat concerned with the 'I can't fly but I can type 80 words per minute' syndrome," said one pilot. Still, about 90% of the pilots saw the glass cockpit as a big step forward.

Evidently, new FAA rules will require more electronics by 1993, to warn of impending collisions and warn of wind shear. The companies that make the electronics seem happy about this new business. Other

future possibilities mentioned include storing flight maps on optical disk, exchanging written messages with flight controllers by 'datalink', and moving to satellite communication and navigation.

The last paragraph mentions that

Another project sounds like it could all but replace the co-pilot. The Air Force boldly calls it the "pilot associate." More than a mere autopilot, the associate devices use artificial intelligence to help fly the plane, plan missions and deploy weapons. The project is in such an early stage that it will take several years to find its way into jet fighters and, eventually, commercial planes.

Note that the concerns expressed in these articles are only about the pilot's own skills decreasing, and not at all about possible mistakes on the part of the computer system. The only reason given for not using fly-by-wire is economic.

John M. Sullivan Princeton Univ. Math Dept.

---

## **✈ India Airlines' A320**

*Subhasish Mazumdar <mazumdar@gaviao.cs.umass.edu>*

*Sun, 4 Mar 90 16:48:31 EST*

Doubts about Indian engineers and RISKS faced by developing countries.

Regarding the A320 crash, George Michaelson <ggm@cc.uq.oz.au> writes:

>Doubts were expressed about the ability of the airline to maintain the

>complex flight control equipment ...

>... it seems from this interview as if the Indian

>engineers themselves question their ability to handle this package.

>                    ^^^^^

Indians are extremely annoyed with the performance of the state-run domestic carrier Indian Airlines, which has a long history of incredible management problems aggravated by political interference. Many Indians would agree with those doubts directed at the ability of \*that airline\*, but few would accept those doubts directed at Indians engineers \*in general\*. This is not the forum to enumerate the technological sophistication that Indians have demonstrated. Suffice it to say that the interpretation of the word \*their\* in George Michaelson's analysis is difficult to swallow.

>I suspect other parallels exist with well-meaning donation/supply of IT

>infrastructure that failed to match local conditions eg lack of tropical

>"hardening", availability of spike-free UPS, spares, training.

You are right here. Often, however, developing countries are taken for a ride! I was involved in the assembly of a Flying Spot Scanner at the Indian Institute of Science, Bangalore, using equipment imported from a reputed company in the UK. One of the crucial power supplies blew up when powered up. We traced the problem to incorrect wiring (the

connections to the collector and emitter of a transistor were reversed, if I remember right). It was evident that the unit \*had never been powered up before shipment\*, let alone tested; but the company refused to admit it, making sly references instead to our lack of training. We gave up the idea of litigation because of the high costs involved. Please think for a moment about the RISKS FACED BY developing countries.

Subhasish Mazumdar, Computer & Information Science, Univ of Massachusetts, Amherst, MA 01003, USA

---

## ✂ Airbus A320: Getting a few things straight

Pete Mellor <pm@cs.city.ac.uk>

Mon, 5 Mar 90 13:33:51 PST

A few misunderstandings seem to be creeping into the debate on the A320. At the risk of adding my own misunderstandings, let me try to clarify a few points raised in [RISKS-9.71](#) by Steve Milunovic and [RISKS-9.72](#) by Robert Dorsett.

Steve Milunovic (9.71) refers to:

> ... a dispute in France over whether the computerized, highly advanced  
> aircraft is too complicated to fly.

One justification for introducing fly-by-wire as in the A320 is that, since most crashes are due to pilot error, a system that reduces the probability of such error will make flying safer. There are two aspects to this:

- Reduction in the pilot's workload.
- Automatically preventing a command from the pilot taking the aircraft out of a 'safe flight envelope', e.g. overriding a command to put the nose up and throttle back if this would cause a stall.

To achieve these aims, the A320 must be EASIER to fly than than its predecessors. It has been argued (I think by one of the pilots' unions) that being trained to fly the A320 does not qualify a pilot to fly a 'traditional' ('fly-by-string'?) aircraft, in the same way that a driving test taken in an automatic does not qualify a motorist to drive a vehicle with a standard\* gearbox.

(The issue of MAINTENANCE, as opposed to flying the aircraft, is a different matter, and I am inclined to agree with Robert Dorsett on this.)

He also refers to a claim that:

> ... the French pilots were opposing it to protect their economic interests.  
> The plane uses two pilots; many other aircraft use three.

To be precise, the crew of a traditional aircraft of the size of the A320 includes a pilot, co-pilot, and flight engineer. The flight engineer's job is to monitor the systems on the aircraft and recover from, or work around, system failures. Along with fly-by-wire, the A320 includes automatic monitoring of

systems with a CRT display of their status to the pilot and co-pilot. The argument is that this reporting system does most of the job of the flight engineer, who is therefore redundant.

Part of the economic justification for the A320 is, therefore:

- Room for one more passenger.
- Save the flight engineer's salary.

It is the French and Australian flight ENGINEERS' unions who have argued most strongly against two-man crews. Their vested interest is obvious, but they have made a strong case on the grounds of safety for the traditional division of labour between flying the plane and watching dials. This case was well presented in a BBC television program in the 'Horizon' series a year or so ago called 'The Essential Third Man'.

(I believe that one inducement that was offered to the pilots was increased rates for two-man crews. I am not sure what the current positions of the various pilots' unions are. If they still oppose the loss of the engineer, I would say it is to their credit.)

Steve also points out:

- > ... as a small note, the flight augmentation system of the 757 is in no way
- > comparable to the A320's fly-by-wire system (or its associated software
- > protections). The former is dedicated to damping aerodynamic instability;
- > the former [latter? - PM] introduces new \*control laws\* and appears to be
- > intended to work around problems involved in the use of side-stick
- > controllers.

Er..., not QUITE. The software in the A320 Electronic Flight Control System (EFCS) is right at the heart of the whole system. The traditional joy-stick between the pilot's legs has been replaced by the side-stick because, since the connection between the pilot and the control surfaces on the wings is electrical rather than mechanical, brute force is no longer necessary to move the controls. The side-stick transmits the commands of the pilot to the EFCS, which processes them together with input from sensors (air-speed indicator, altimeter, etc.) and sends signals to the effectors governing the control surfaces.

The 'control laws' define how this processing is done. They are implemented as tables of parameters. There are several sets of laws, each controlling a particular mode of flight (take-off, cruising, landing, etc.). I am puzzled by Robert Dorsett's aside:

- >... (that is, above 100', beneath which the protections disappear).

The protections CANNOT disappear at any altitude, however low. Perhaps he means that at this phase of the flight a different set of control laws come into force. Robert quite correctly states that:

- > Airbus proper regards "manual" (electric horizontal stabilizer trim and
- > manual rudder) backup as a last-ditch emergency system. Numerous reports
- > indicate that its operation isn't even part of the standard Airbus training
- > curriculum.

I believe they train to use manual backup on a simulator. I believe also that an actual landing using manual backup has been demonstrated by a test pilot, but that the ability to do such a landing was not required as part of the type certification. The EFCS is 'flight-critical' (if it fails under certain circumstances it could result in a catastrophic accident), but not FULL-TIME flight-critical (its availability need not be 100%, since the mechanical backup will enable the aircraft to cruise straight and level while the system is rebooted).

Whatever the details, however, the point is that there is NO WAY that the A320 would be flown on a commercial flight without the EFCS, except in an emergency.

He goes on to say:

> Upon examination, various terms could be examined [You can say that again!-PM]  
> --perhaps "manual" means hand-flying it (with protections) to the ground,  
> rather than tracking an ILS.

I'm inclined to agree. This confusion over the meaning of "manual" also bedeviled the accounts of the previous crash.

The point of the slow fly-past at the Mulhouse-Habsheim air show was to demonstrate the ability of the EFCS to fly the aircraft very close to stalling without actually doing so. Without such an automatic system, such a manoeuvre simply would not be possible. Loose statements to the effect that the automatic system was 'switched off' for the demonstration are nonsense. What probably WAS done was to set up the EFCS so that cruise 'control laws' still applied at low altitude, but this is pure speculation on my part, and I should not open my mouth too wide without hard information as a backup.

To avoid rambling on ad nauseam, I will make two last points:

- The EFCS is not the only flight-critical software controlled system on the A320. The Full-Authority Digital Engine Control (FADEC) is just as vital, and obviously must act in cooperation with the EFCS. I have a fair amount of information on the fault-tolerant hardware and software architecture of the EFCS, but I do not know of anything that has been published about the FADEC.
- The overriding concern regarding type-certification of fly-by-wire is our continuing inability to certify systems containing software to high levels of reliability. FAA and CAA regulations (taken in conjunction with explanatory memos) require that a flight-critical system must have a demonstrated probability of failure no greater than  $10^{-9}$  per flying hour in a flight of mean duration. The same set of documents state that no means exist of assigning such a probability number to software-induced failure. Certification in this case largely rests on the demonstration of adherence to a development process standard (RTCA-DOC/178A), together with provision of fault-tolerance.

It is this latter anomaly that research should address urgently.

\*Note for US readers: A vehicle with a standard gearbox has a third pedal called the 'clutch', and a wobbly lever next to the driver's seat which has to be moved every time you change speed.

Peter Mellor, Centre for Software Reliability, City University,  
Northampton Square, London EC1V 0HB Tel.: +44 (0)1-253-4399 Ext. 4162/3/1

---

### **✂ Mileage Plus wants me to move**

*Tim Kay <tim@through.cs.caltech.edu>*

*Wed, 28 Feb 90 11:13:29 pst*

Mileage Plus is United's travel bank. I can redeem miles traveled on United Airlines along with dollars spent on my Mileage Plus Visa card for free travel rewards.

I just finished a conversation with a United Mileage Plus representative, informing her for the FIFTH time that my zip code is 91125 rather than 91102. Each time their computer changes the zip code back to 91102 in a way that they cannot override. I get no mail from them.

The problem is that Caltech has its own zip code. My address is

Tim Kay, Caltech, 256-80, Pasadena, CA 91125

The representative checked further and explained that their computer "knows" that Pasadena doesn't have a 91125 zip code. (They then somehow come up with 91102 totally bogus; 91106 is the surrounding zip code.) Could I please give them my home address instead? No, I don't check my mail box at home.

She had no further suggestions. I guess I'd have to stop using their services until I move!

I suggested we try

Tim Kay, Box 256-80, Caltech, CA 91125

I can't wait to see what happens.

Tim

---

### **✂ Credit-card fraud [previously in misc.security; RISKS-relevant too]**

*Douglas Mason <douglas@ddsw1.mcs.com>*

*Thu, 1 Mar 90 20:26 CST*

Something interesting that I heard was going on at [eastern college] was that a couple of students were able to get a hold of a credit-card magnetic strip recorder somehow. They also stole purses, wallets, anything that they could get their hands on that had credit cards in it.

After doing the above, they would dig through dumpsters (we all know that

story) and pick up carbons or other receipts that have credit card numbers on them, and make a list of valid card numbers.

Using the encoding machine, they then erased the old card number off of the magnetic strip (which had probably been reported stolen by this time) and encoded on that same strip one of the card numbers that they had picked up out of the dumpsters.

So now they have say a MasterCard with an invalid number embossed on the front of it, and a different-but-valid account on the magnetic strip. What good is this? Plenty good for the clever thief!

They then went into shopping malls or anywhere that the credit-card validation machines were the all-too-familiar "slide the card through and read the number off the mag strip" type.

The merchant would authorize the card successfully and get an approval code, then run the card though and get a paper receipt. The merchants never check the card number on the authorization machine display and compare it to that of the card!

When the merchants send in the credit card slips to the bank, they of course come back, and I imagine it takes a long time to figure out what exactly happened.

Merchants beware!

-Douglas Mason

Douglas T. Mason          douglas@ddsw1.mcs.com or dtmason@m-net.UUCP



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

**Volume 9: Issue 74**

**Monday 12 March 1990**

## Contents

- [Airbus Crash: Reports from the Indian Press](#)  
[N. Balaji](#)
- [Indian Airlines A320 in the German press](#)  
[Udo Voges](#)
- [The C3 legacy, Part 4: A gaggle of L-systems](#)  
[Les Earnest](#)
- [The risks of keeping old versions -- Daigle book](#)  
[Graeme Hirst/David Sherman](#)
- [PSU Hackers thwarted](#)  
[Angela Marie Thomas](#)
- [Anonymous Word Processing: `Z'](#)  
[Jon von Zelowitz](#)
- [Re: Now Prodigy Can Read You](#)  
[Eric Roskos](#)
- [Re: Traffic System Failure](#)  
[Peter Ahrens](#)
- [Tracking criminals and the DRUG police-action](#)  
[J. Eric Townsend](#)
- [Human-Centered Automation](#)  
[Robert Dorsett](#)
- [Drive-by-wire cars](#)  
[Craig Leres](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✉ **Airbus Crash: Reports from the Indian Press**

*N. Balaji <balaji@redwood.USC.EDU>  
Fri, 9 Mar 90 20:02:42 PST*

Below are excerpts from three reports related to the Feb. 14th Airbus crash which appeared in the weekly edition of The Statesman, an English language newspaper published from Calcutta and New Delhi.

Madras [India], Feb 17. -- An Indian Airlines A-320 aircraft, on a

scheduled flight from here to Bangalore this morning, developed a snag in mid-air and was brought back safely.

When the aircraft was airborne for 20 minutes and was halfway to Bangalore, there was a drop in cabin pressure and passengers complained of suffocation. It was flown back and grounded and the passengers were transferred to a Boeing-737 and flown to Bangalore.

The day after the A-320 aircraft crashed in Bangalore [on Feb. 14] killing 90 passengers one of the engines of another A-320 Airbus failed as the aircraft was getting ready for take-off from Begum airport in Hyderabad for Madras. The flight was aborted.

Alarmed by the frequent snags, Indian Airlines pilots are wary of flying the A-320 Airbus, the most sophisticated civilian aircraft anywhere in the world.

The fly-by-wire system of computer-driven controls used in the A-320 is common to Mirage-2000 fighter planes also. The Indian Air Force has built air-conditioned hangars in Gwalior for its Mirage fleet but Indian Airlines has not even provided ordinary hangars for its A-320 aircraft. Two of its grounded A-320 were parked in the open for two months, one in Bombay and the other in Delhi, exposed to heat, dust and moisture. ...

[On Feb. 18, the Civil Aviation Ministry grounded all 14 Airbus aircraft in the Indian Airlines fleet pending an official inquiry. Delivery of 12 more A-320 aircraft on order has also been suspended. -nb]

New Delhi, Feb. 15. -- Preliminary investigations into the Airbus crash at Bangalore yesterday are reported to be focusing on the sudden drop in height of the aircraft as it was on its final approach for landing at the runway of the airport, reports PTI [Press Trust of India].

According to Civil Aviation Ministry sources here today, there was no distress signal from the pilot to the control tower and the aircraft appeared set for a smooth landing before the sudden drop under clear weather conditions.

The sources said it was possible that the pilot either misjudged the height at which he was flying or he was misled by the instruments on board...

Bangalore, Feb. 14. -- ...

[The Civil Aviation Minister Arif Mohammad Khan] said the pilot [Captain S. S. Gopujkar, who was in command of the flight] was one of the most experienced in Indian Airlines and even manufacturers of the Airbus had placed him in the "excellent pilot" category after he underwent training. "He was flying the aircraft and it is a mystery how the accident happened", Mr Khan said.

[See, in contrast, the report translated from Badische Neueste Nachrichten 22

Feb 90 by Udo Voges in [Risks 9.70](#). - nb]

The following is from Indian Abroad, March 2, 1990, published from New York.

New Delhi -- Even as the Airbus Industrie launched a campaign to undermine [sic] the expertise of Indian Airlines' Airbus pilots in the French media, the Indian government continued to persist with its apprehensions about the aircraft.

A technical committee armed with comprehensive terms of reference began a probe into the whole Airbus affair last week. ...

The five-member expert committee announced by Civil Aviation Minister Arif Mohammed Khan, would go into Indian Airlines' state of preparedness to safely operate the Airbus. ...

The issue of the Airbus' safety has become a national one with important newspapers making editorial comments. The Indian press has urged the Indian government to thoroughly examine the safety aspects of the plane before allowing [it] to fly once again. ...

---

### ✂ Re: A320 ([Risks 9.70](#))

*Udo Voges <voges@idtuva.uucp>  
Fri, 9 Mar 90 08:37:11 +0100*

Pilot to blame for Airbus-Crash  
(translated from Badische Neueste Nachrichten, 9 March 1990)

Paris (dpa). The crash of an Airbus A320 in India in mid February, in which 90 people were killed, is due to carelessness of the pilot. This was found after analysis of the tape from the cockpit. In Paris it was announced, that the function of the airplane was not in question. According to the announcement, the analysis of the tape showed that the pilot of the crashed airplane of Indian Airlines was training the copilot during landing. In the course of this he didn't pay sufficient attention that the airplane should keep its required speed. This was announced from well-informed French sources. The Indian Government has gotten a preliminary report, in which the reopening of the use of the Indian A320 is recommended.

---

### ✂ The C3 legacy, Part 4: A gaggle of L-systems

*Les Earnest <LES@SAIL.Stanford.EDU>  
05 Mar 90 2025 PST*

Martin Minow contributes some SAGE anecdotes in [RISKS 9.68](#), including the following.

- > My friend also mentioned that the graphics system could be used to display
- > pictures of young women that were somewhat unrelated to national defense
- > -- unless one takes a very long view -- with the light pen being used
- > to select articles of clothing that were considered inappropriate in the

> mind of the viewer. (Predating the "look and feel" of MacPlaymate by  
> almost 30 years.) Perhaps Les could expand on this; paying special  
> consideration to the risks involved in this type of programming.

While light pens did exist in that period, SAGE actually used light  
\_guns\_, complete with pistol grip and trigger, in keeping with military  
traditions. Interceptors were assigned to bomber targets on the large  
displays by "shooting" them in a manner similar to photoelectric arcade  
games of that era.

Regrettably, I never witnessed the precursor to MacPlaymate, which  
probably appeared after my involvement. While I never saw anything bare  
on the SAGE displays, a colleague (Ed Fredkin) did stir up some trouble by  
displaying a large Bear (a Soviet bomber of that era) as a vector drawing  
that flew across the screen. Unfortunately, he neglected to deal with X, Y  
register overflow properly, so it eventually overflowed its address space.  
The resulting collision with the edge of the world produced some bizarre  
imagery, as distorted pieces of the plane came drifting back across the  
screen.

(Continuing from [RISKS 9.67](#))

A horde of command-control development projects was initiated by the Air  
Force in the early 1960s. Most were given names and each was assigned a  
unique three digit code followed by "L." Naturally, they came to be  
called "L-systems." A Program Manager (usually a Colonel) was put  
in charge of each one to ensure that financial expenditure goals were met.  
Those who consistently spent exactly the amounts that had been planned  
were rewarded with larger sums in succeeding budgets. Monthly management  
reviews almost never touched on technical issues and never discussed  
operational performance -- it was made clear that the objective was to  
spend all available funds by the end of the fiscal year and that nobody  
cared much about technical or functional accomplishments.

In 1960, after earlier switching from MIT Lincoln Lab to Mitre Corp., my  
group was assigned to provide technical advice to a Colonel M., who was in  
charge of System 438L. This system was intended to automate the  
collection and dissemination of military intelligence information. Unlike  
most command-control systems of that era, it did not have a descriptive  
name that anyone used -- the intelligence folks preferred cryptic  
designations, so the various subsystems being developed under this program  
were generally called just "438L."

I had recently done a Masters thesis at MIT in the field of artificial  
intelligence and hoped to find applications in this new endeavor. I soon  
learned that the three kinds of intelligence have very little in common  
(i.e. human, artificial, and military).

IBM was the system contractor for 438L and was already at work on an  
intelligence database system for the Strategic Air Command Headquarters  
near Omaha. They were using an IBM 7090 computer with about 30 tape  
drives to store a massive database. It turned out to be a dismal failure  
because of a foreseeable variant of the GIGO problem, as discussed below.

The IBM 438L group had also developed specifications for a smaller system that was to be developed for other sites. Colonel M. asked us to review the computer Request for Proposals that they had prepared. He said that he planned to buy the computer sole-source rather than putting it out for bids on the grounds that there was "only one suitable computer available." When I read it, there was no need to guess which computer he had in mind -- the RFP was essentially a description of the IBM 1410, a byte-serial, variable word length machine of that era.

When Colonel M. sought my concurrence on the sole-source procurement, I demurred, saying there were at least a half-dozen computers that could do that job. I offered to prepare a report on the principal alternatives, including an approximate ranking of their relative performance on the database task. He appeared vexed, but accepted my offer.

My group subsequently reviewed alternative computers and concluded that the best choice, taking into account performance and price, was the Bendix G-20. I reported this informally to Colonel M. and said that we would write it up, but he said not to bother. He indicated that he was very disappointed in this development, saying that it was not reasonable to expect his contractor (IBM) to work with a machine made by another company. I argued that a system contractor should be prepared to work with whatever is the best equipment for the job, but Col. M seemed unconvinced.

This led to a stalemate; Colonel M. said that he was "studying" the question of how to proceed, but nothing further happened for about a year. Finally, just before I moved to another project, I mentioned that the IBM 1410 appeared to be capable of doing the specified task, even though it was not the best choice. Col. M. apparently concluded that I would not make trouble if he proceeded with his plan. I later learned that he initiated a sole-source procurement from IBM just two hours after that conversation.

In the meantime, the development project at SAC Headquarters was falling progressively further behind schedule. We talked over this problem in my group and one fellow who had done some IBM 709 programming remarked that he thought he could put together some machine language macros rather quickly that would do the job. True to his word, this hacker got a query system going in one day! I foolishly bragged about this to the manager of the IBM group a short time later. Two weeks after that I discovered that he had recruited my hotshot programmer and immediately shipped him to Omaha. I learned to be more circumspect in my remarks thereafter.

The IBM 438L group did eventually deliver an operable database system to SAC, but turned out to be useless because of GIGO phenomena (garbage in, garbage out). Actually, it was slightly more complicated than that. Let's call it GIGOLO -- Garbage In, Gobbledygook Obliterated, Late Output.

The basic problem was that in order to build a structured database, the input data had to be checked and errors corrected. In this batch environment, the tasks of data entry, error checking, correction, and file

updating took several days, which meant that the operational database was always several days out of date.

The manual system that this was supposed to replace was based on people reading reports and collecting data summaries on paper and grease pencil displays. That system was generally up-to-date and provided swift answers to questions because the Sergeant on duty usually had the answers to the most likely questions already in his head or at his finger-tips. So much for the speed advantage of computers!

After several months of operation with the new computer system, the embarrassing discovery was made that no questions were being asked of it. The SAC senior staff solved this problem by ordering each duty officer to ask at least two questions of the 438L system operators during each shift. After several more months of operation we noted that the total number of queries had been exactly two times the number of shifts in that period.

The fundamental problem with the SAC 438L system was that the latency involved in creating a database from slightly buggy data exceeded the useful life of the data. The designers should have figured that out going in, but instead they plodded away at creating this expensive and useless system. On the Air Force management side, the practice of hiring a computer manufacturer to do system design, including the specification of what kind of computer to buy, involved a clear conflict-of-interest, though that didn't seem to worry anyone.

(Next segment: Subsystem I)

-Les Earnest (Les@Sail.Stanford.edu)

---

## ✂ The risks of keeping old versions

*Graeme Hirst <gh@ai.toronto.edu>*

*Sat, 10 Mar 90 16:03:59 EST*

>From the Toronto /Globe and Mail/, 9 March 90:

The much-hyped launch of Chantale Daigle's\* book took a bizarre twist yesterday as the publisher ordered that all 40,000 copies be burned and a corrected version be issued.

``We made a serious technical error. We printed the working copy of the (computer) disc instead of the final, edited version," said Monique Summerside, a spokesman [sic] for Les Editions 7 Jours Inc. She said that the changes to be made were strictly grammatical and typographical, and were not due to the threat of a lawsuit. ``This is very embarrassing and even more expensive, but we have a obligation to the public to provide a good product."

. . . The book was scheduled to go on sale yesterday . . . but distribution was delayed until Monday because of the recall.

[\*Chantale Daigle was at the centre of a controversial Canadian court case concerning abortion last year.]

[A Toronto Star article from the same day was submitted by David Sherman, dave@lsuc.on.ca, who wondered how likely would it have been for a printer to accidentally print from an earlier draft when using pre-computer printing methods? Probably much more difficult, especially if type were involved -- the old version was simply not around anymore! But it would have been just as easy in the old days to lose the marked-up proof pages... PGN]

---

## PSU Hackers thwarted

Angela Marie Thomas <thomas@shire.cs.psu.edu>  
Sat, 10 Mar 90 00:22:22 GMT

The Daily Collegian Wednesday, 21 Feb 1990

Unlawful computer use leads to arrests  
ALEX H. LIEBER, Collegian Staff Writer

Two men face charges of unlawful computer use, theft of services in a preliminary hearing scheduled for this morning at the Centre County Court of Common Pleas in Bellefonte. David Geyer, 234 S. Allen St., and Robert W. Clark, 201 Twin Lake Drive, Gettysburg, were arrested Friday in connection with illegal use of the University computer system, according to court records. Geyer, 36, is charged with the theft of service, unlawful computer use and criminal conspiracy. Clark, 20, is charged with multiple counts of unlawful computer use and theft of service. [...]

Clark, who faces the more serious felony charges, allegedly used two computer accounts without authorization from the Center of Academic Computing or the Computer Science Department and, while creating two files, erased a file from the system. [...] When interviewed by University Police Services, Clark stated in the police report that the file deleted contained lists of various groups under the name of "ETZGREEK." Clark said the erasure was accidental, resulting from an override in the file when he tried to copy it over onto a blank file. According to records, Clark is accused of running up more than \$1000 in his use of the computer account. Geyer is accused of running up more than \$800 of computer time.

Police began to investigate allegations of illegal computer use in November when Joe Lambert, head of the university's computer department, told police a group of people was accessing University computer accounts and then using those accounts to gain access to other computer systems. Among the systems accessed was Internet, a series of computers hooked to computer systems in industry, education and the military, according to records.

The alleged illegal use of the accounts was originally investigated by a Computer Emergency Response Team at Carnegie-Mellon University, which assists other worldwide computer systems in investigating improper computer use.

Matt Crawford, technical contact in the University of Chicago computer department discovered someone had been using a computer account from Penn State to access the University of Chicago computer system.

---

### **✂ Anonymous Word Processing: `Z'**

*Jon von Zelowitz <vonzelow@adobe.com>*

*Thu, 8 Mar 90 18:22:42 PST*

In [RISKS 9.71](#), R. Clayton quotes an article in the New Republic which gave astounding "evidence" for the attribution of an anonymous article based on claimed textual correspondence between it and a file on a computer. (I assume that Clayton's submission was concerned with the lack of security of the computer file.) The New Republic article said:

The staff member called up the file on his own computer during our interview and read me lengthy passages, all of which were identical to passages in "To the Stalin Mausoleum" [the title of the Daedalus article].

What kind of evidence is this? Even if the reporter had personally seen the file on the screen, it means nothing. File ownership is easily faked. And since passages were read to the reporter, it was probably a telephone interview. "Yes, I've got the article right here on my computer screen..." Wow. I have a bridge to sell to that reporter.

Jon von Zelowitz ...sun!adobe!vonzelow vonzelow@adobe.com

---

### **✂ Re: Now Prodigy Can Read You ([RISKS-9.69](#))**

*Eric Roskos <jer@ida.org>*

*Fri, 09 Mar 90 09:37:19 E*

In [Risks 9.69](#), Donald B. Weschler writes:

> The Prodigy system accesses remote subscribers' disks to check the  
> Prodigy software version used, and when necessary, downloads the latest  
> programs. ... I asked Prodigy how they protect against the possibility  
> of altering subscribers' non-Prodigy programs, or reading their personal  
> data. ... According to Prodigy, the feature cannot be disabled.

This issue was debated at length on the PRODIGY service several months ago; an explanation was given by Harold Goldes, one of the PRODIGY service's more technically knowledgeable user-support people. The "programs" updated by the PRODIGY software are not executable files loadable by the PC's operating system; it is not even clear that it is code executable by the PC's CPU. Rather, routines to draw the individual graphics displays used by the PRODIGY software are cached on the user's disk in a single file, STAGE.DAT, and this cache is updated via normal cache-updating algorithms. The PRODIGY software is unable to update the DOS-executable object programs automatically, and has to send

out new disks when this is necessary. The explanation given in the \_PRODIGY\_Star\_ newsletter was an overly-abbreviated version, limited in technical detail by the PRODIGY service's orientation to nontechnical people, and, no doubt, by space limitations.

Nevertheless, due the PC's lack of security mechanisms, the possibility of altering subscriber's programs or reading personal data does exist on any such system. PRODIGY representatives have repeatedly stated that the PRODIGY software will not do this, and my examination of the operation of the software has not shown any evidence that any file other than STAGE.DAT is updated.

A topic that has not been so clearly answered is what some users feel to be the PRODIGY service's overuse of its built-in censorship facilities and its employment of "over 100" censors; they feel the PRODIGY service uses this facility to control the expression of opinions on the service's bulletin boards which may adversely affect marketing goals.

[PRODIGY is a trademark of Prodigy Services Company, a partnership of IBM and Sears.]

---

### **✦ Re: Traffic System Failure (Rich Neitzel, [RISKS-9.73](#))**

<prahrens@pttesac.UUCP>  
Thu, 8 Mar 90 10:47:12 -0800

> ... you could immobilize a major urban area ...

Perhaps it would not be trivial to point out that Norman Spinrad published a story in Analog about 25 years ago which used this exact scenario, wherein a foreign power immobilises New York City.

-Peter Ahrens, San Francisco

---

### **✦ Tracking criminals and the DRUG police-action**

J. Eric Townsend <jet@karazm.math.uh.edu>  
Sun, 11 Mar 90 15:24:29 CDT

>From the Communications of the ACM, vol. 33, no. 3, March 1990:

"News Track:

DRUG WARS... A new FBI computer system created to monitor the activities of suspected drug traffickers may eventually be able to predict their next move. Drawing information from several existing FBI databases, the "Drug Information System" lists suspects' names and stores data on their cars, travel, phone calls, meetings, assets, and family connections. Its monitor can display fingerprints, mugshots and surveillance photos. By year-end, AI capabilities will be added to help agents detect suspicious actions, suggest leads and forecast crimes. The system will be installed in four cities by the end of the

month, and 18 cities by the end of the year."

"forecast crimes" -- could they have predicted the hit and run driver who totaled my car and didn't even stop to check if my passenger and I were injured? Maybe they should try predicting crimes by politicians and federate employes first, just to get the bugs out of the system....

No :-).

J. Eric Townsend, University of Houston Dept. of Mathematics (713) 749-2120

---

## **✂ Human-Centered Automation**

*Robert Dorsett <rd@rascal.ics.utexas.edu>*

*Mon, 5 Mar 90 16:46:31 CST*

From: AirLine Pilot, February 1990:

### **NASA BUILDING TECHNOLOGY BASE FOR HUMAN-CENTERED AUTOMATION**

NASA has launched a research program aimed at improving aviation safety by developing and applying what it calls "human-centered automation" for flight crews and air traffic controllers. The agency hopes to develop, by 1994, a design for both a cockpit and a controller station that are both intelligent and human centered.

According to NASA documents developed for a recent NASA conference on aviation safety and automation, the agency's goal is to "provide the technology base leading to improved safety of th national airspace system through development and integration of human-centered automation technologies for aircraft crews and air traffic controllers."

Automation, says NASA, "can improve the efficiency, capacity, and dependability of the national aviation system." But, the agency acknowledges, \*humans\* will manage, operate, and assure the safety of the next-generation system. Therefore, "human-centered automation is the key to effectiveness."

The specific objectives of the NASA program are to:

- \* develop philosophies and guidelines for applying human-centered automation to the flight deck and to ATC controller stations;
- \* Provide for flight crews human-centered automation concepts that "ensure full situational awareness"; and
- \* provide for air traffic controllers human-centered automation concepts and methods that "allow integration and management of information and air-ground communications."

The program has three main elements:

The element dealing with "human/autoamtion interaction" will treat such

subjects as a methodology for analyzing human error, ways of measuring work-load, and "functional validation of intelligent systems."

A program element on intelligent error-tolerant systems will evaluate collision avoidance systems, "smart" checklists, weather displays, a cockpit procedures monitor, and more.

A third program element, concerned with ATC/cockpit integration, will look at pilot/controller communications management, enroute flow management and scheduling, final approach spacing, and similar issues.

---

### Drive-by-wire cars

*Craig Leres <leres@helios.ee.lbl.gov>  
Sat, 03 Mar 90 18:26:11 PST*

There was an interesting article in the January issue of Car and Driver magazine titled the "Ten Best Things To Come." One of the ten things is drive-by-wire. They discuss some of the issues some of the issues applicable to both fly and drive by wire:

"Obviously, a primary concern with drive-by-wire systems is reliability and fail-safe operation."

There's a picture of a electronically controlled throttle; the PC board says BOSCH on it and the hardware appears to be the upper assembly of a carburetor, i.e. there's a servo which control a throttle plate. This may be the unit used in the BMW 750iL which is claimed to be the only example of a drive by wire automobile on the American market.

The systems they expect us to see in the future will control not only the throttle but steering and suspension. Examples include four wheel steering and dynamic camber adjustment.

Hopefully, auto manufacturers will be as conservative with drive by wire systems as they have been with the computer controlled engines they are current building. For example, the engine in my '89 GM car has a computer that controls functions such as fuel delivery and ignition. But nearly all the computer controlled systems have backups that implement the "limp home mode." There's an oil pressure switch which activates the electric fuel pump should the computer fail to. The ignition system has a backup circuit that takes over if the computer stops supplying ignition timing data.

Craig



Search RISKS using [swish-e](#)

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





Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

**Volume 9: Issue 75**

**Thursday 15 March 1990**

## Contents

- [PRODIGY updating programs](#)  
[Simson L. Garfinkel](#)
- [Who shall guard the guards?](#)  
[Robert A. Levene](#)
- [Journalistic hacking](#)  
[Rodney Hoffman](#)
- [Caller-id by name](#)  
[Gary T. Marx](#)
- [Re: PSU Hackers thwarted](#)  
[David C Lawrence](#)
- [Re: Tracking criminals and the DRUG police-action](#)  
[Brinton Cooper](#)
- [RISKS of "Evolutionary Software"](#)  
[Rajnish and Gene Spafford via Will Martin](#)
- [Human-centered automation](#)  
[Donald A Norman](#)
- [Re: Airbus Crash: Reports from the Indian Press](#)  
[Henry Spencer](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **PRODIGY updating programs**

*Simson L. Garfinkel <simsong@prose.CAMBRIDGE.MA.US>  
12 Mar 90 20:44:07 EST (Mon)*

I must take issue with Eric Roskos saying that PRODIGY can only update information in the STAGE.DAT file.

In doing my article on PRODIGY for The Christian Science Monitor, I was told by Prodigy's manager of software services that one of the really nifty tricks of PRODIGY is that nearly the entire system running on the PC --- including the .EXE files --- can be updated remotely. This eliminates the need to send out floppy disks with updates. (They didn't have it working well at the beginning and actually had to send out one update --- an extremely expensive

proposition.)

The reason for wanting to do this is based on two things: prodigy's pricing structure and its target market. Prodigy charges one \$9.95 a month. At that price, it just isn't possible to economically send out floppy disks. Especially if they want to have 1-5 million subscribers within the next 2-10 years.

The other thing is their target market: they want people who don't know anything about programs or files. Automatic updates eliminate the necessity of having to have users put disks into their computers and try to figure out what is going on.

The Prodigy censors is a very real problem. They have recently shut down PRODIGY groups that have ventured into "unacceptable" topics like abortion and homosexuality.

---

### ✂ Who shall guard the guards? (was: Drive-by-wire cars)

Robert A. Levene <levene@aplcomm.jhuapl.edu>

Wed, 14 Mar 90 13:00:49 EST

In [RISKS 9.74](#) Craig Leres <leres@helios.ee.lbl.gov> writes:

> ... Hopefully, auto manufacturers will be as conservative with drive by wire  
> systems as they have been with the computer controlled engines they are  
> currently building. For example, the engine in my '89 GM car has a computer  
> that controls functions such as fuel delivery and ignition. But nearly all  
> the computer controlled systems have backups that implement the "limp home  
> mode." ...

Don't let an acute failure mode lull you into a false sense of security. My 8500-mile '89 GM car is in a dealer's repair shop due to computer failure. If the emissions computer \*fails\*, the car will "limp home." But if an erratic computer misinterprets the car's state, it will send faulty control signals and cause unpredictable performance. "Hey, HAL - Can you say 'Garbage In, Garbage Out?'"

For two weeks, the computer failed intermittently, occasionally stalling the car without warning - not a pleasant experience, especially when it stalled while going 55mph on a 10-lane highway, and at a busy intersection while making a turn. After several such failures and three tows, the car's computer finally failed for the mechanics, giving them the required justification to replace the computer.

The computer already has the capability to detect faulty sensors throughout the engine. A second, independent computer is needed to monitor the performance of the engine computer (i.e., "guard the guards") in order to detect and record intermittent failures. At minimum, the car should also have a manual override switch to enter "limp home" mode instead of the \$45 "tow home" mode.

Rob Levene

---

## **✂ Journalistic hacking**

*Rodney Hoffman <Hoffman.ElSegundo@Xerox.com>*

*11 Mar 90 18:24:20 PST (Sunday)*

Summarized from a story by Sheryl Stolberg in the 'Los Angeles Times' 10 March 1990:

Fox Television employees in New York and Los Angeles discovered in February that someone had been trying to gain access to their computers, using the same password in both cases.

Free-lance journalist Stuart Goldman was arraigned Friday and charged with violating federal and California anti-hacking laws. His personal computer and floppy disks were confiscated. According to the federal prosecutor's affidavit, Goldman made several attempts -- at least one of them successful -- to gain entry to "sensitive data files regarding ... news stories worked upon by the company's journalists."

Network officials would not disclose what information was sought, but Goldman had worked briefly for the Fox-produced news tabloid 'A Current Affair', and he had recently been trying to sell an inside story on such shows to the 'Los Angeles Times'.

[See 'Hacking for a competitive edge' in [RISKS 8.71](#) for an earlier case of journalists apparently trying to steal stories via computer hacking.]

---

## **✂ Caller-id by name**

*<gtmarx@ATHENA.MIT.EDU>*

*Tue, 13 Mar 90 14:48:59 EST*

Newsday, February 27, 1990

Don't Give Up Your Privacy to Find Out Who's Calling

Gary T. Marx

The telephone is something that is usually answered, but rarely questioned. But this is changing with the proposal of the regional phone companies to introduce unblockable Caller ID.

Almost everyone answers "yes" to the question "Would you like to know who is calling you before you pick up the phone?" But most people would answer "no" to the corollary question, "Would you mind if every time you made a call your phone number was automatically revealed to the person called?"

This offering, for which the phone company would charge a separate fee, changes the nature of phone service by removing the control that callers have over their phone numbers. In other words, the service has consequences for the

person calling -- unlike other recent developments in phone service, such as speed dialing or automatic redialing.

By technological fiat, the phone company takes personal information away from the caller and sells it to the person called. This is similar to the data scavenging companies that sell credit and related information about individuals without their consent. Contrary to what most people believe, the phone companies are saying they, not you, control your phone number.

Unblockable Caller ID is unlikely to become the standard in the United States. California already has a law requiring that if the service is offered, it should come with a free blocking option -- callers not wanting to reveal their number can enter three digits and the called party will see a "P" for private call. Similar federal legislation has been introduced in Congress by Senator Herbert H. Kohl (D-Wisc).

That is the compromise position. Don't ban the service. Don't offer it in an unrestricted way as most phone companies propose. Give callers limited control over what is revealed - -their number, or the fact that they don't want to reveal it.

While such a position is better than an unrestricted offering, it is far from ideal. Callers not wanting to reveal their number to the person called run the risk of not getting through. People receiving calls, seeing a "P" may decide that if you won't identify yourself, they won't talk to you. That is a reasonable response on the part of the called person seeking to avoid unwanted calls. The caller appears suspect - -even though in most cases what callers wish to keep to themselves is their phone number and perhaps location, not their name.

The problem is that now, as proposed, the only form of identification the technology delivers is the phone number. If it were changed so that callers had the option of delivering their names, most privacy problems would be resolved. In general it would also be more useful to the people called to see a name rather than a phone number. They needn't run the risk of refusing a call from an unrecognized phone number that might in fact be a family member calling from a service station to report the car has broken down, or a surprise visit from a out-of-town friend. This is also normal phone etiquette, which begins with callers identifying themselves by name, not by telephone number.

One would hope that the phone companies, as publicly regulated monopolies would feel an obligation to develop technical innovations that, beyond enhancing profits, would further important social values such as privacy and equity.

At a minimum, their actions should not diminish these as unblockable Caller ID will. Investors, systems designers, and marketers need to consider how a development might be misused, or have undesirable social consequences.

Services like Caller ID should be developed in consultation with citizen advisory groups. Consumers should not be put in the defensive position of having to respond to whatever radical changes the local phone service proposes.

We live in a democracy, not a technocracy. As networks become more important and as invasive technologies more powerful, public utility commissions which

traditionally have focused on the economic aspects must look to broader social aspects. Too often, communications technology is seen only as something that erodes, rather than enhances, privacy. But that need not be the case. Giving callers the option of providing their name would serve the interests of both the caller and the person called.

---

**✉ Re: PSU Hackers thwarted (Angela Marie Thomas, [RISKS-9.74](#))**

David C Lawrence <tale@turing.cs.rpi.edu>

Tue, 13 Mar 90 10:12:38 EST

Just a couple of comments on this story. These aren't criticisms but just perspective observations; as professionals in all areas of life discover there are frequently some differences of opinion about how matters of their field should be presented to the general populace. Recognising that these differences spring up even between members of the field, these are my opinions.

According to records, Clark is accused of running up more than \$1000 in his use of the computer account. Geyer is accused of running up more than \$800 of computer time.

As a user of several systems that use pseudo-monetary accounting schemes, I question whether any resources were really wasted at all, "computer time"-wise. I do not know much about the systems in question, but if they parallel those that I have had these experiences with then there were cycles to spare. To me, just handing out numbers with dollar signs attached seems to be attempting to (either knowingly or not; I do not know the author's experience, either) garner a response of, "So much money! The waste! Clearly a terrible degree of theft!"

Among the systems accessed was Internet, a series of computers hooked to computer systems in industry, education and the military, according to records.

Everytime I see comment about the Internet like this it just makes me ponder what the general public thinks. Is it, "OH! Some terribly important network! Our national security might have been breached!"? I do not mock the importance of the Internet. The reality of the Internet, though, is that access to it is something that many people can get quite easily through their school or work and the fact that the Internet was "Among the systems accessed" isn't a very shocking thing. Then again, perhaps it is shocking based on the system he was coming from. My comment, however, is based on what general reaction to the above statement could be like -- the public won't know about the specifics of that system either.

Matt Crawford, technical contact in the University of Chicago computer department discovered someone had been using a computer account from Penn State to access the University of Chicago computer system.

Not to detract from Matt's work, but this paragraph essentially says nothing. One of the reasons that these networks exist is so that people can do work at a

machine when they are half-way around the world from it. There is nothing especially surprising about someone from one university accessing a computer at another university. This is lacking in information and only makes me wonder what we are supposed to infer from it.

Dave

---

**✂ Re: Tracking criminals and the DRUG police-action ([RISKS-9.74](#))**

*Brinton Cooper <abc@BRL.MIL>*

*Tue, 13 Mar 90 9:02:04 EST*

In [Risks 9.74](#), J. Eric Townsend writes, in part:

- > "forecast crimes" -- could they have predicted the hit and run driver
- > who totaled my car and didn't even stop to check if my passenger and
- > I were injured? Maybe they should try predicting crimes by politicians
- > and federate [sic] employes [sic] first, just to get the bugs out of
- > the system....

I presume he meant "federal employees". In any case, his statement is an unwarranted defamation of the character of literally millions of public employees who work honestly, cheerfully, and carefully to give the taxpayer's an honest day's work for a fraction of an honest day's pay. As an academic, Mr (Dr?) Townsend should be a little more objective in his characterization of folks who work in other domains.

\_Brint

---

**✂ RISKS of "Evolutionary Software" (Rajnish, Spafford)**

*Will Martin <wmartin@STL-06SIMA.ARMY.MIL>*

*Fri, 9 Mar 90 8:41:35 CST*

The following is extracted from the latest issue of the Computers and Society Digest. Please note the comments about this software "growing" to become so complex that it can no longer be understood by its creators. As soon as I read that, I thought of "Risks"!

Regards, Will Martin

\*\*\*Begin Extract\*\*\*

The Computers and Society Digest, Volume 4, #9  
Thursday, March 8th 1990

From: "rajnish" <KJ16@MARISTB.BITNET>

Date: Wed, 28 Feb 90 10:49:32 PST

Subject: Evolutionary Software?

I was wondering what people thought of the Darwinian software being created by the computer scientists at the University of California in Los Angeles?

Their approach is pretty radical and they're creating more powerful and reliable software through self-evolution than their programmers can design by hand.

I guess these small modular programs they have going interact and merge with each other to create new generations that can anticipate potential pitfalls that human programmers can't. Just like we humans think about so many things at the same time in our head, the computer runs thousands of programs simultaneously and a master program picks out the ones that suits its' needs most efficiently, integrating it to produce following generations that are even more powerful. Survival of the fittest?

In Alameda and Orange Counties in California, an example of their Darwinian programming is helping the county to control their mosquito population. Each of the individual program modules are able to successfully mimic the behavior of the mosquitoes to determine growth rate, etc., to find out precisely where and how much insecticide is necessary to kill itself and its' children. Instead of the previous mass insecticide bombings at 20000 sites picked out by human programmers, this software is doing a near perfect job with only 3000 sites it picked out on its' own. Pretty impressive, you think?

The computer scientist who developed this approach to software design, Danny Hillis (Founder of Thinking Machines in Cambridge, Mass.) thinks because of its constant evolution that his software is eventually going to make itself so complex that even their designers won't be able to comprehend all of its' functions. Kinda like becoming God?

This guy even has software working like a biological parasite to wipe out incompetent programs and therefore forcing the master program to search for programs that are even better! This parasite even looks around for viruses to kill. Instead of taking the usual route, trying to simulate human qualities like vision and speech, Hallis' artificial intelligence is just trying to mimic unexpected behavior that all organisms exhibit and using a parallel supercomputer to accelerate the natural evolutionary process as defined by Darwin.

Interesting, you think? Rajnish

-----

Date: 3 Mar 90 23:30:30 GMT  
From: spaf@cs.purdue.edu (Gene Spafford)  
Subject: Re: Evolutionary Software?

Danny Hillis presented his work at the 2nd Conference on Artificial Life, held in Santa Fe, the week of Feb. 4. Lots of other interesting ideas were presented, too.

The proceedings of the 1st conference have been published by Addison-Wesley. The second set of proceedings will be published next year, also by Addison-Wesley.

You can get more information about the conference by contacting Chris Langton @ the Santa Fe Institute for Non-linear Studies, (505) 667-1444.

(I was there, talking about computer viruses as a form of artificial life.)

Gene Spafford

\*\*\*End extract\*\*\*

---

## ✂ Human-centered automation

*Donald A Norman-UCSD Cog Sci Dept <danorman@UCSD.EDU>*

*Thu, 15 Mar 90 08:10:33 PST*

[RISKS 9.74](#) had a statement about the NASA human-centered aviation safety project. I don't know if I am in that project, but

1. Ed Hutchins and I have a grant with NASA-Ames on aviation safety.
2. I have strongly argued for user-centered system design (UCSD) in general.
3. We are working on the checklist problem and on the automation problem.

So a quick summary of our work might be appropriate: it certainly fits the domain covered by RISKS.

Automation. I have been concerned with the fact that too many automatic devices are built not only to take over the jobs performed by humans, but with no understanding of the issues that will arise when they fail. A simple example is the Air China incident in which the number 4 engine lost power, and the autopilot compensated without notifying anyone. If the 1st officer had been flying instead of the autopilot, he might have said "hmm, I seem to be compensating more and more. Wonder what's happening?" But the autopilot was silent, and when the problem finally exceeded the control authority of the autopilot, the result was an uncontrolled aircraft that almost was a total disaster.

I have analyzed this and other aviation incidents in a tech report that is available upon request. Abstract at the end of this note.

Checklists. In our opinion, a checklist is an admission that humans fail. After all, if we didn't we wouldn't need to check. Therefore, appropriate design of equipment and procedures can probably eliminate or at least reduce the need for checklists.

We don't need a checklist to ensure that we open the door before passing through it -- unless it is a glass door. We used to try to start our autos without first inserting the key in the ignition switch, but now that the starter key and the ignition key are the same, we no longer make that error. Wiener and Asani point out that pilots sometimes take off without lowering their flaps (so there is a warning buzzer and it is a checklist item), but they never land without lowering flaps, so this condition need not be checked for. In similar fashion, the takeoff checklist has all sorts of items on it, but NOT to advance throttles. Yes it seems obvious, but that is just the point.

Except for a study by Wiener and Asani that is just now being completed (for NASA-Ames) there have been NO systematic analyses of the scientific/cognitive bases of checklists. They are now constructed by a combination of the intuitions of chief pilots, experience, and the concerns of the legal staff. Lists for the same aircraft in different airlines vary dramatically. This is a real safety hazard: read the NTSB reports on the Delta Dallas crash and the Northwestern Detroit crash.

Hutchins and I are doing a cognitive analysis of checklists. We will have a paper "any month now."

Automated checklists can help, but

1. They are not the final answer.
2. Locating them on a front-panel CRT is probably the wrong way to go.
3. They have to be designed with an understanding of human cognition.
4. Checklists, procedures, and do-lists should probably be combined.

===

Abstract of tech report

The "Problem" of Automation: Inappropriate Feedback and Interaction,  
Not "Over-Automation"

As automation increasingly takes its place in industry, especially high-risk industry, it is often blamed for causing harm and increasing the chance of human error when failures occur. I propose that the problem is not the presence of automation, but rather its inappropriate design. The problem is that the operations under normal operating conditions are performed appropriately, but there is inadequate feedback and interaction with the humans who must control the overall conduct of the task. When the situations exceed the capabilities of the automatic equipment, then the inadequate feedback leads to difficulties for the human controllers.

The problem, I suggest, is that the automation is at an intermediate level of intelligence, powerful enough to take over control that used to be done by people, but not powerful enough to handle all abnormalities. Moreover, its level of intelligence is insufficient to provide the continual, appropriate feedback that occurs naturally among human operators. This is the source of the current difficulties. To solve this problem, the automation should either be made less intelligent or more so, but the current level is quite inappropriate.

The overall message is that it is possible to reduce error through appropriate design considerations. Appropriate design should assume the existence of error, it should continually provide feedback, it should continually interact with operators in an effective manner, and it should allow for the worst of situations. What is needed is a soft, compliant technology, not a rigid, formal one.

Norman, D. A. (1990). The "problem" of automation: Inappropriate feedback and interaction, not "over-automation". *Philosophical Transactions of the Royal Society of London, B* (Paper prepared for the Discussion Meeting, "Human Factors in High-Risk Situations," The Royal Society (Great Britain),

June 28 & 29, 1989.)

Don Norman, Department of Cognitive Science D-015, University of California,  
San Diego, La Jolla, California 92093 USA

---

**✈ Re: Airbus Crash: Reports from the Indian Press**

<henry@zoo.toronto.edu>

Thu, 15 Mar 90 14:52:31 EST

- > A technical committee armed with comprehensive terms of reference
- > began a probe into the whole Airbus affair last week. ...

Interestingly enough, it looks like somebody in authority at least suspected that the results would be embarrassing to the airline (i.e. mismaintenance or pilot error rather than technical problems). Normally, in such an accident investigation, the airworthiness authorities of the aircraft's country of origin -- i.e., the people who first certified the thing as flyable -- are involved, and the manufacturer is at least kept informed. Aviation Week reports that India refused European airworthiness authorities' request to participate, and also refused information requests from them and from Airbus Industrie.

Henry Spencer at U of Toronto Zoology  
uunet!attcan!utzoo!henry henry@zoo.toronto.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 9: Issue 76

Monday 19 March 1990

## Contents

- [How history gets made, or, myths spread like viruses at the CVIA](#)  
[Doug McIlroy](#)
- [London Underground wrong-way train in rush-hour](#)  
[Brian Randell](#)
- [Privacy in Printout](#)  
[L. P. Levine](#)
- [Send it by FedEx = Don't Send It At All!](#)  
[Betsy Perry](#)
- [20th Int. Symp. on Fault-Tolerant Computing](#)  
[Neil Speirs](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **How history gets made, or, myths spread like viruses at the CVIA**

<[doug@research.att.com](mailto:doug@research.att.com)>

Sun, 18 Mar 90 22:37:12 EST

When Time magazine was writing their 1988 cover story on viruses, I sent them a copy of Ken Thompson's Turing lecture, which detailed an early and particularly secretive and patient one (a computer "slow virus"?) that he had demonstrated but had not allowed to spread. The conclusion of the lecture was a strongly worded warning about the rise of computer vandalism and worse, and advice to all who would listen that "brilliant" is rarely the right adjective for such activities.

In the interview with Time, I had also discussed "Darwin", a game of survival of the fittest among self-reproducing programs, which Vyssotsky, Morris, and I had played sometime around 1962. Darwin had been described in the computer recreation column of Software - Practice and Experience in 1972. Rechristening it "core wars", Kee Dewdney popularized it in Scientific American in 1984.

More interested in a good story than an accurate one, Time's writer made up a wheeze about the Bell Labs folks having kept the awful

secret of self-reproducing programs to themselves, with the pact of silence being broken by the Turing Lecture. Probably because it didn't fit with the thesis that Ken let the cat out of the bag, the Time article was silent about Ken's admonitory message.

Now Ken McAfee, self-styled "leading expert" and principal in the Computer Virus Industry Association, and Colin Hayes, "investigative reporter", have enshrined Time's sensationalism in their book on viruses. They simplify the myth even further, implying that Ken talked about core wars - a trifling subject compared to what he really did describe. Apparently McAfee and Hayes, having found a good story in Time, never looked further, certainly not at the Turing lecture, which is hardly an obscure reference.

The investigative reporter did eliminate some of Time's errors: he didn't misspell Vyssotsky's name and mine, but probably only because he identified us merely as "young AT&T programmers". Instead, out of nowhere, he decided that we were "engaged in the groundwork for artificial intelligence." Perhaps I underestimate his ability to misread the record. He may believe in Vyssotsky's chaostron.

Doug McIlroy, Bell Labs

[The 1959 Chaostron piece reappeared most recently in the Communications of the ACM, vol 27, no 4, April 1984, pp. 356-7, in a section entitled "An Anthology of Selections Spanning 25 Years", in an issue whose table of contents page mysteriously says "May 1984"! For those of you who haven't seen it, this item is an absolute classic. PGN]

---

## London Underground wrong-way train in rush-hour

Brian Randell <Brian.Randell@newcastle.ac.uk>  
Fri, 16 Mar 90 17:30:16 BST

Following on from recent discussions in RISKS about railway signalling, I thought it appropriate to submit the attached article, which appeared in the Financial Times on Thursday, 15 March 1990. (It is reprinted in its entirety without permission.) I'm alarmed that London Transport do not seem to have thought before of the sort of situation described. I'm also intrigued that the manner in which a disaster was avoided is also implied to be novel - if this is really so then the train driver showed amazing presence of mind.

Brian Randell

### RUSH HOUR TRAIN DRIVEN WRONG WAY UP TUNNEL

By Roy Hodson

An empty London underground train was driven along a tunnel in the wrong direction towards a train packed with passengers during last Monday evening's rush-hour at 6pm in an incident that London

Underground is now giving the priority of a major disaster.

The driver of the empty train became disoriented after being told to manoeuvre the train to a cross-over point. The signalling system was unable to cope as he set off north instead of south on the Piccadilly Line from Kings Cross.

The rogue train was stopped just 400 feet from a stationary train crammed with 800 passengers.

Kings Cross was the scene of a fire disaster on November 18, 1987 in which 31 people were killed.

Disaster was averted in this new incident by the prompt action of the driver of the stationary train. He saw approaching train lights and reached through his window to seize some 12-volt telephone wires, shorting the circuit.

A programme is now going on throughout the underground network to redesign parts of the signalling system. Work will be completed by the weekend. Fifty stationary red lights are being fitted at points identified as possible accident sites, of a similar accident.

"The present signalling system cannot understand that a train is going backwards in a one-way tunnel", a London Underground manager said last night. "The new lights will warn a driver in the remote possibility of this ever happening again".

Brian Randell, Computing Laboratory, University of Newcastle upon Tyne, UK

---

## **Privacy in Printout**

*Prof. L. P. Levine <len@cvax.cs.uwm.edu>  
Mon, 19 Mar 90 11:02:58 CDT*

Is TDD printed output Information or just paper?

>From the Milwaukee Journal, 3/18/90.

A piece of TDD (Telecommunication Device for the Deaf) output was pried from the clenched fist of a deaf man, resulting in a life prison sentence for murder, according to an appeal being considered by the Wisconsin Supreme Court.

The questions created by this case include: Was the paper obtained illegally? Is the TDD output to be considered public information or as private as a phone conversation? Since the TDD was in the sheriff's department office in Pierce County, Wisconsin, the paper is police property. Is the information written on it during normal use also police property?

The facts of the case: Robert Rewolinski was picked up on a traffic charge in June 1987. He used the TDD in the sheriff's office to call his common law wife, Catherine Teeters, for a ride home. During the TDD conversation Teeters

told Rewolinski "I am scared like hell you will do something to me or the kids. I don't want the kids to have short lives or hurt... I can't stand you anymore... You must understand that I don't want you and I don't love you."

Three hours later the sheriff's TDD received a call with the message "Robert Rewolinski here. Lost my mind. Cathy's dead." The TDD printout of the earlier conversation was considered the critical evidence in convicting him of first degree murder rather than manslaughter. The prosecution contends that the deputy was simply retaining custody and control of police property. She could not have been looking for evidence of a crime since no crime had yet been committed. The defense contends Rewolinski deserves a new trial because the printout should not have been taken or used as evidence.

It is clear that the paper belonged to the sheriff. Did the information on it belong to them too? The police do not monitor phone conversations in such circumstances, how about TDD communication?

Leonard P. Levine, Professor, Computer Science, Univ. Wisconsin-Milwaukee

---

### **✉ Send it by FedEx = Don't Send It At All!**

*Betsy Perry <betsyp@apollo.com>*

*Fri, 16 Mar 90 10:46:11 EST*

Thought you might be amused by my latest encounter with Bad Computer Programming. Last Saturday, I phone-ordered a selection of seeds from Shepherd's Seeds in Connecticut. I asked that the seeds be sent Second Day Air, since planting season is coming fast. The salesperson said "Sure, I'll mark it FedEx; that'll be \$5.00 extra.", and we parted with mutual expressions of esteem.

Five days later, on Thursday, I called Shepherd's to enquire why the seeds hadn't arrived. After the order-taker had done some quick computer-sleuthing, she came up with a shamefaced explanation. Their computerized order-entry system schedules orders to be filled based on the method of shipping; normally, 2nd Day Air orders are scheduled to be filled on the evening of arrival. Unfortunately, my order-taker had marked the order "FedEx". Since Shepherd's never ships seeds by Federal Express (they use UPS exclusively), the order-entry system never scheduled my order to be shipped. Presumably, my order would have languished unfilled until the Judgment Day, or until Shepherd's switched delivery services.

---

### **✉ 20th Int. Symp. on Fault-Tolerant Computing**

*Neil Speirs <Neil.Speirs@newcastle.ac.uk>*

*Mon, 19 Mar 90 14:41:16 GMT*

The Twentieth International Symposium on Fault-Tolerant Computing (FTCS-20)

26-28th June, 1990

Newcastle Crest Hotel, New Bridge Street, Newcastle upon Tyne, UK

Sponsored by: Computer Society of the IEEE, CSR, BCS, IEE, ESPRIT,  
University of Newcastle upon Tyne, IFIP Working Group 10.4.

FTCS is the international symposium on fault-tolerant systems. It is devoted to state-of-the-art issues in fault tolerant computing and encompasses all aspects of specifying, designing, modelling, implementing, testing, diagnosing and evaluating dependable and fault-tolerant computing systems and their components. In addition to a full programme of contributed papers, invited talks will be given on two very significant and interesting systems, each of which has extremely challenging dependability requirements, in the areas of banking and air traffic control, respectively.

The Association for Payment Clearing Service's CHAPS system provides the UK same-day guaranteed electronic credit transfer service for 14 settlement banks and over 300 participant banks. The transaction value often exceeds 80 billion pounds per day. This system will be described by Mr Eryl Thomas, who has overall responsibility for the operation of CHAPS, together with Mr Jim Reeves, CHAPS Technical Manager, and Mr Geoff Birks, a Senior Manager with the IT Planning Department of the National Westminster Bank, which is a major CHAPS user.

Dr Flaviu Cristian, who is on the staff of the IBM Research Center, Almaden, California, will describe plans for the Advanced Automation System (AAS). The AAS system is being built for the US Federal Aviation Authority, as a total replacement for the existing North American air traffic control system. The AAS contract, whose total value is 3.55 billion dollars, is the biggest single contract in IBM's history, and the biggest non-military procurement by the US Government ever. Dr Cristian has just received a Corporate Award (IBM's highest technical award) for his key contributions to the design of the AAS.

Further information and enquires regarding registration should be made to:  
FTCS-20 REGISTRATION, Keepers Lodge, Great Chart, Kent TN26 1JX, UK.,  
Tel. +44 23 382 258.



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

**Volume 9: Issue 77**

**Wednesday 21 March 1990**

## Contents

- [Stranded Satellite](#)  
[Steve Bellovin](#)
- [Re: London Underground wrong-way train in rush-hour](#)  
[Richard A. Schumacher](#)
- [Internet Intruder \(John Markoff via PGN excerpted\)](#)
- [Internet Intruder Warning](#)  
[J. Paul Holbrook](#)
- [Risks of reporting breakins](#)  
[Randal Schwartz](#)
- [Re: Privacy in Printout](#)  
[Tim Wood](#)  
[Henry Spencer](#)
- [Computer-based phones threaten privacy \(again!\)](#)  
["34AEJ7D"](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **Stranded Satellite**

<[smb@ulysses.att.com](mailto:smb@ulysses.att.com)>

Tue, 20 Mar 90 13:34:34 EST

An attempt to launch the \$150M Intelsat 6 communications satellite from a Titan 3 rocket failed recently because of a wiring error in the booster. The problem was compounded by a human communications failure between the electricians and the programmers.

The rocket was wired in a two-satellite configuration. This was erroneous; only one satellite was aboard that rocket. The command to separate the satellite from the booster rocket was generated by a computer; however, when the computer people said that they would launch the "first" payload, they meant the top one, while the the wiring people understood "first" to mean the bottom payload compartment -- which wasn't used. And -- if I attempt to translate the newspaperese back into technical English -- it appears that the

separation signal had to travel through the satellite to reach the separation device; given the faulty wiring, it didn't pass through.

[Subsequent firing of liquid-fueled rocket thrusters has gotten the satellite into a higher orbit, where it may be safe (but still not usable) for a few extra months. PGN]

---

**✉ Re: London Underground wrong-way train in rush-hour ([RISKS-9.76](#))**

*Richard A. Schumacher <schumach%convex@uunet.UU.NET>  
21 Mar 90 00:58:01 GMT*

The article seems to suggest that train drivers on the Underground have control over the switchwork (!). Can this possibly be true?

---

**✉ Internet Intruders**

*John Markoff via PGN (excerpted) <neumann@csl.sri.com>  
21 Mar 90 10:30:41*

SELF-PROCLAIMED 'HACKER' SENDS MESSAGE TO CRITICS  
By JOHN MARKOFF, c.1990 N.Y. Times News Service

A man identifying himself as the intruder who illegally penetrated part of a nationwide computer linkup said Tuesday that he had done so to taunt computer security specialists who have denounced activities like his. His assertion came in a telephone call to The New York Times on Tuesday afternoon. The man identified himself only as an Australian named Dave, and his account could not be confirmed. But he offered a multitude of details about various electronic break-ins in recent months that were corroborated by several targets of the intruder. He said he was calling from outside the United States, but that could not be verified.

Federal investigators have said that in recent months the intruder has illegally entered computers at dozens of institutions in a nationwide network, the Internet. Once inside the computers, they said, the intruder stole lists of the passwords that allow users to enter the system and then erased files to conceal himself. [...]

Investigators in the new Internet case said the federal authorities in Chicago were close to finding the intruder and several associates. The U.S. attorney's office in Chicago refused to confirm that assertion. The investigators said that in some cases the intruder might have used a program that scanned the network for computers that were vulnerable.

In his telephone call to The Times on Tuesday, the man said he had broad access to U.S. computer systems because of security flaws in those machines. As a self-proclaimed computer hacker, he said, he decided to break in to the computer security experts' systems as a challenge. Among the targets of the recent attacks were Clifford Stoll, a computer system manager at the Smithsonian Astronomical Observatory at Harvard University, and Eugene Spafford, a computer scientist who specializes in computer security issues at Purdue University. The caller said he was upset by Stoll's portrayal of intruders in a new book, "The Cuckoo's Egg." "I was angry at his

description of a lot of people," the caller said. "He was going on about how he hates all hackers, and he gave pretty much of a one-sided view of who hackers are."

Several days ago the intruder illegally entered a computer Stoll manages at Harvard University and changed a standard welcome message to read: "Have Cliff read his mail. The cuckoo has egg on his face. Anonymous." The caller explained in detail his techniques for illegally entering computer systems. He gave information about Stoll's and Spafford's computer systems that matched details they were familiar with.

And he described a break-in at an external computer that links different networks at Digital Equipment Corp. A spokeswoman for the company confirmed that a machine had been entered in the manner the caller described. But the caller was not able to penetrate more secure Digital computers, she said.

The caller said he had intended to tease the security experts but not to damage the systems he entered. "It used to be the security guys chase the hackers," he said. "Now it's the hackers chase the security people."

Several managers of computer systems that were entered said that no significant harm had been done but that the invader had wasted the time of system administrators, who were forced to drop their normal duties to deal with the breaches in security.

Ordinary users were also inconvenienced, the managers said, because their computers had to be temporarily removed from the system for security reasons.

Investigators familiar with the break-ins said the intruder had entered systems by using several well-known security flaws that have been widely distributed in computerized mailing lists circulated among systems managers.

Stoll, who from 1986 to 1988 tracked a group of West Germans breaking into U.S. corporate, university and nonclassified military computers, said the intruders had not proved any point. "It's sad that people have these gunslinger ethics," he said. "It shows how easy it is to break into even a modestly secure system." Spafford, who has also written <garbled>, but added that nothing significant had been compromised. [...]

As a result of the break-ins, the Smithsonian Astronomical disconnected its computers from the Internet, a network that connects servers around the world.

Among the institutions believed to have been penetrated by the intruder are the Los Alamos National Laboratory, Harvard, Digital Equipment, Livermore Laboratories, Boston University and the University of Texas.

Tuesday, the caller asserted that he had successfully entered dozens of different computers by copying the password files to his machine and then running a special program to decode the files. That program was originally written as a computer security experiment by a California-based computer scientist and then distributed to other scientists. [... reference to the following CERT message...]

Asked Tuesday whether he would continue his illegal activities, the caller said he might lay low for a while. "It's getting a bit hot," he said, "and we went a bit berserk in the past week."

---

### Internet Intruder Warning

"J. Paul Holbrook" <ph@CERT.SEI.CMU.EDU>

Mon, 19 Mar 90 15:42:52 EST

CA-90:02

CERT Advisory

March 19, 1990

Internet Intruder Warning

There have been a number of media reports stemming from a March 19 New York Times article entitled 'Computer System Intruder Plucks Passwords and Avoids Detection.' The article referred to a program that attempts to get into computers around the Internet.

At this point, the Computer Emergency Response Team Coordination Center (CERT/CC) does not have hard evidence that there is such a program. What we have seen are several persistent attempts on systems using known security vulnerabilities. All of these vulnerabilities have been previously reported. Some national news agencies have referred to a 'virus' on the Internet; the information we have now indicates that this is NOT true. What we have seen and can confirm is an intruder making persistent attempts to get into Internet systems.

It is possible that a program may be discovered. However, all the techniques used in these attempts have also been used, in the past, by intruders probing systems manually.

As of the morning of March 19, we know of several systems that have been broken into and several dozen more attempts made on Thursday and Friday, March 15 and 16.

Systems administrators should be aware that many systems around the Internet may have these vulnerabilities, and intruders know how to exploit them. To avoid security breaches in the future, we recommend that all system administrators check for the kinds of problems noted in this message.

The rest of this advisory describes problems with system configurations that we have seen intruders using. In particular, the intruders attempted to exploit problems in Berkeley BSD derived UNIX systems and have attacked DEC VMS systems. In the advisory below, points 1 through 12 deal with Unix, points 13 and 14 deal with the VMS attacks.

If you have questions about a particular problem, please get in touch with your vendor.

The CERT makes copies of past advisories available via anonymous FTP (see the end of this message). Administrators may wish to review these as well.

We've had reports of intruders attempting to exploit the following areas:

1) Use TFTP (Trivial File Transfer Protocol) to steal password files.

To test your system for this vulnerability, connect to your system using TFTP and try 'get /etc/motd'. If you can do this, anyone else can get your password file as well. To avoid this problem, disable tftpd.

In conjunction with this, encourage your users to choose passwords that are difficult to guess (e.g. words that are not contained in any dictionary of

words of any language; no proper nouns, including names of "famous" real or imaginary characters; no acronyms that are common to computer professionals; no simple variations of first or last name, etc.) Furthermore, inform your users not to leave any clear text username/password information in files on any system.

If an intruder can get a password file, he/she will usually take it to another machine and run password guessing programs on it. These programs involve large dictionary searches and run quickly even on slow machines. The experience of many sites is that most systems that do not put any controls on the types of passwords used probably have at least one password that can be guessed.

2) Exploit accounts without passwords or known passwords (accounts with vendor supplied default passwords are favorites). Also uses finger to get account names and then tries simple passwords.

Scan your password file for extra UID 0 accounts, accounts with no password, or new entries in the password file. Always change vendor supplied default passwords when you install new system software.

3) Exploit holes in sendmail.

Make sure you are running the latest sendmail from your vendor. BSD 5.61 fixes all known holes that the intruder is using.

4) Exploit bugs in old versions of FTP; exploit mis-configured anonymous FTP

Make sure you are running the most recent version of FTP which is the Berkeley version 4.163 of Nov. 8 1988. Check with your vendor for information on configuration upgrades. Also check your anonymous FTP configuration. It is important to follow the instructions provided with the operating system to properly configure the files available through anonymous ftp (e.g., file permissions, ownership, group, etc.). Note especially that you should not use your system's standard password file as the password file for FTP.

5) Exploit the finger hole used by the Morris Internet worm.

Make sure you're running a recent version of finger. Numerous Berkeley BSD derived versions of UNIX were vulnerable.

Some other things to check for:

6) Check user's .rhosts files and the /etc/hosts.equiv files for systems outside your domain. Make sure all hosts in these files are authorized and that the files are not world-writable.

7) Examine all the files that are run by cron and at. We've seen intruders

leave back doors in files run from cron or submitted to at. These techniques can let the intruder back on the system even after you've kicked him/her off. Also, verify that all files/programs referenced (directly or indirectly) by the cron and at jobs, and the job files themselves, are not world-writable.

8) If your machine supports uucp, check the L.cmds file to see if they've added extra commands and that it is owned by root (not by uucp!) and world-readable. Also, the L.sys file should not be world-readable or world-writable.

9) Examine the /usr/lib/aliases (mail alias) file for unauthorized entries. Some alias files include an alias named 'uudecode'; if this alias exists on your system, and you are not explicitly using it, then it should be removed.

10) Look for hidden files (files that start with a period and are normally not shown by ls) with odd names and/or setuid capabilities, as these can be used to "hide" information or privileged (setuid root) programs, including /bin/sh. Names such as '.. ' (dot dot space space), '...', and .xx have been used, as have ordinary looking names such as '.mail'. Places to look include especially /tmp, /usr/tmp, and hidden directories (frequently within users' home directories).

11) Check the integrity of critical system programs such as su, login, and telnet. Use a known, good copy of the program, such as the original distribution media and compare it with the program you are running.

12) Older versions of systems often have security vulnerabilities that are well known to intruders. One of the best defenses against problems is to upgrade to the latest version of your vendor's system.

#### VMS SYSTEM ATTACKS:

13) The intruder exploits system default passwords that have not been changed since installation. Make sure to change all default passwords when the software is installed. The intruder also guesses simple user passwords. See point 1 above for suggestions on choosing good passwords.

14) If the intruder gets into a system, often the programs loginout.exe and show.exe are modified. Check these programs against the files found in your distribution media.

If you believe that your system has been compromised, contact CERT via telephone or e-mail.

J. Paul Holbrook, Computer Emergency Response Team (CERT), Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213-3890  
Internet E-mail: [cert@cert.sei.cmu.edu](mailto:cert@cert.sei.cmu.edu)  
Telephone: 412-268-7090 24-hour hotline: CERT personnel answer  
7:30a.m.-6:00p.m. EST, on call for emergencies  
other hours.

Past advisories and other information are available for anonymous ftp from [cert.sei.cmu.edu](http://cert.sei.cmu.edu) (128.237.253.5).

## ✂ Risks of reporting breakins

Randal Schwartz <merlyn@iwarp.intel.com>

Tue, 20 Mar 90 09:15:32 PST

"Who *\*was\** that bearded man?"

Just Peter Neumann, the RISKS moderator. He was being interviewed on CNN last night about the recent Internet breakins.

Now for the RISKS element:

The reporter, while talking about "hacker-this" and "virus-that", used screen shots of a terminal. The text was obviously from some BSD-like system, because I recognized a listing of /etc. A moment later, for at least two seconds on the screen, I got a clear picture of /etc/passwd! And a few moments later, an entire login sequence (with hostname, username, and password)! (I wasn't taping it... sigh. :-)

When you let the press into your cube, be sure you aren't doing something wonderful on your screen.

Does this qualify as an "out-of-band" transmission? :-)

Randal L. Schwartz, Stonehenge Consulting Services Beaverton, Oregon, USA  
(503)777-0095

[Good point, although it occurred at least once before on a filmed episode of a lady hacker being shown carrying out a breakin on camera. PGN]

---

## ✂ Re: Privacy in Printout ([RISKS-9.76](#))

Tim Wood <tim@sybase.com>

Tue, 20 Mar 90 18:00:44 PST

It seems to me that the crux of this very disturbing story is whether or not the defendant had a reasonable expectation of privacy in using the Police Dept.'s TDD. That expectation is governed by the physical surroundings, assuming there is no electronic monitoring of the telephone or TDD call. Are arrestees' telephone/TDD conversations that take place in the sheriff's office understood to be off-limits to the police?

A telephone caller in an occupied room would risk at least his side of the conversation being overheard; a TDD caller would risk a department employee looking over his shoulder to read the printed dialogue.

The occupied-room situation seems to offer no expectation of privacy for either type of call, less for the TDD than for phone. If, however, the defendant had a reasonable expectation of privacy, then it would seem to be basic discrimination against deaf people to use physical evidence of a private conversation (the printed text itself) to prove a more serious charge, since no such physical evidence would exist for an ordinary phone conversation. The

printout (paper + content) may be police property, but there are many cases where certain police property or knowledge is not admitted as evidence.

Note that the US Supreme Court recently ruled that users of cordless telephones have no reasonable expectation of privacy. Thus if the conversation took place over such a phone, the conversation, whether spoken or TDD, seemingly could have been recorded and used as evidence. -TW

Sybase, Inc. / 6475 Christie Ave. / Emeryville, CA / 94608 415-596-3500

---

### **✂ Re: Privacy in Printout ([RISKS-9.76](#))**

<henry@zoo.toronto.edu>

Tue, 20 Mar 90 11:48:14 EST

A somewhat similar question has been settled and may perhaps provide some guidance: who owns a (physical, not electronic) letter? The issue comes up in connection with publication of "collected letters of J. Doe" books and the like. The way this has generally been resolved is that the addressee owns the physical copy of the letter, but the sender (or his heir) owns the copyright on the contents.

Henry Spencer at U of Toronto Zoology

---

### **✂ Computer-based phones threaten privacy (again!)**

<34AEJ7D@CMUVM.BITNET>

Mon, 19 Mar 90 15:38:05 EST

Several universities with computer-based phone systems here in MI have announced that they have in place, or intend to have in place, call tracking systems which will provide printouts for each employee's phone of ALL LOCAL CALLS (as well as long distance) including listing the number called, date and time of the call, and the duration thereof. The privacy implications of all this, and the attendant threat and capacity for abuse, are obvious.



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

**Volume 9: Issue 78**

**Thursday 5 April 1990**

## Contents

- [RAF Tornado collision](#)  
[Dorothy R. Graham](#) via PGN
- [New Georgia Automobile Tags](#)  
[Warren Tucker](#)
- [British tax tales](#)  
[Bob Gray](#) via [Mark Brader](#)
- [Oslo Day in Norway? No way!](#)  
[Paul Dorey](#)
- [Computer backorder on cover letters](#)  
[Yuri Rubinsky](#)
- [London Underground driver's action](#)  
[Martyn Ould](#)
- [Hi-Tech Loo](#)  
[Wayne W. Lui](#) via [Brian Randell](#)
- [Proposed UK Authority for Risk Management](#)  
[Brian Randell](#)
- [More on Prodigy's Updating of a User's Disks](#)  
[Eric Roskos](#)  
[Paul Eggert](#)
- [April Fools Day on the net](#)  
[D. Waitzman](#) via [Martin Minow](#)
- [Automated Fast Food](#)  
[Dave Curry](#)
- [UNIX Trix](#)  
[Paul Eggert](#)
- [Re: PSU Hackers thwarted](#)  
[Pete Mellor](#)
- [Three Australians indicted for computer tampering](#)  
[PGN](#)
- [Info on RISKS \(comp.risks\)](#)

---

✉ **RAF Tornado collision (sent by Dorothy R. Graham)**

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

*Thu, 5 Apr 1990 9:40:14 PDT*

In August 1988 two RAF Tornado fighters collided over the village of Millburn in Cumbria, UK, killing the four crewman. Originating from different airfields, each plane was using the SAME preprogrammed cassette to control its on-board computer in low-altitude flight, which resulted in their both coming together at the same height at the same location at the same time. The MoD report identified an "extraordinary" series of coincidences, and put the blame on insufficient coordination among different RAF bases. New rules have been established.

Source: The (London) Sunday Times, 11 March 1990, excerpting a Ministry of Defence report. Thanks to Dorothy R. Graham for clipping it.

---

### **✂ New Georgia Automobile Tags**

*Warren Tucker <wht@n4hgf.gatech.edu>*

*Thu, 29 Mar 90 00:01:31 EST*

I heard on a local radio station this afternoon that many Georgia Citizens are being erroneously arrested out of state for possession of stolen vehicles. It seems that numbers in the new series license tags (issued since January) sometimes :- ) match numbers from the previous series. Unfortunately for many people, some match numbers belonging to vehicles stolen as long ago as 1983. One elderly gentleman was arrested for riding his own motorcycle. A couple spent the night in an Indiana jail for driving their own car. The state motor vehicle people say they'll get NCIC information updated by September. Adds new meaning to the slogan "Stay and See Georgia," doesn't it?

Warren Tucker, TuckerWare

[Ray Houghton of Augusta GA sent me a clipping  
from the Augusta Chronicle, 27 March 1990. PGN]

---

### **✂ British tax tales**

*Mark Brader <msb@sq.com>*

*Fri, 30 Mar 90 05:17:01 EST*

The following items were forwarded to Usenet's soc.culture.british by Bob Gray (bob@castle.ed.ac.uk), having originally appeared on Oracle. For those who don't know, the term "poll tax" is used in Britain for a new, flat "per head" tax, replacing what we call property taxes; it has nothing to do with voting.

[reformatted]

Student Andrew Mursell, 19, of Ryde, Isle of Wight, expected to pay 70 pounds in poll tax but has just received a bill for nearly 4,000,000 pounds. Medina Council said it was a computing error.

A man waiting for a bus at Maidstone, Kent, was stunned when a postman tried to force him to take a poll tax demand. The letter was addressed to The Occupier, Bus Stop, High Street. "The postman said he tried to give it to the man at the front of the bus queue, but he refused to take it, and I can't blame him," said a council official. "It was all down to a computer error.""

[The second case was also noted by Dave Horsfall <dave@stcns3.stc.oz.au> in Australia! Small world. PGN]

---

### ✂ Oslo Day in Norway? No way!

Paul Dorey <pgd@cix.UUCP>  
Tue Mar 27 21:45:28 1990

The 'Daily Telegraph' of Tuesday March 27th reports a Reuter news agency story:

" A Norwegian Bank was embarrassed yesterday after a cashpoint computer apparently applied its own form of 'fuzzy logic' and handed out thousands of pounds no one had asked for. A long queue formed at the Oslo cashpoint after news spread that customers were receiving 10 times what they requested. "

Paul Dorey (pgd@cix.cix.ukc)

---

### ✂ Computer backorder on cover letters

Yuri Rubinsky <yuri@sq.com>  
Sat, 24 Mar 90 15:35:18 EST

After I stopped by this company's booth at the recent CD-ROM conference, the following letter arrived here from a major CPU manufacturer...

Dear Mr. Rubinsky:

Thank you for your [company name] literature order.

We are very sorry, but the following items that you have requested are currently on backorder:

PRODUCT CODE	DESCRIPTION	EXPECTED ARRIVAL DATE
T217	DEAR CUSTOMER COVER LETTER	FOUR WEEKS

Your order will be filled at the earliest possible date. In the meantime, your patience in regard to this matter is greatly appreciated.

Please feel free to call our Literature Distribution Center at [800-number]. Our operators will be happy to help you place an order for any additional literature, or refer you to your nearest [company

name] sales office to help you with any technical questions regarding our products. If you call to check the status of your order, please reference your order #[number].

Again, thank you for your order, and we hope to be of service to you in the future.

Sincerely,

[empty space here]

[company name]

Literature Distribution Center

Curiously, one week earlier I received the literature I had requested -- without a cover letter.

Submitted to comp.risks and rec.humor.funny by Yuri Rubinsky, SoftQuad Inc., 720 Spadina Ave., Toronto, Ontario, Canada M5S 2T9

---

### **✂ London Underground driver's action ([RISKS-9.76](#))**

*Martyn Ould <mao@praxis.UUCP>*

*Mon, 26 Mar 90 12:05:45 BST*

I heard an interview with the driver of the train shortly after he had averted the accident. As I remember it, he said that he had seen the train approaching him at speed from behind and had taken the action he was trained to take, namely to short circuit a particular circuit. It sounded, the way he put it, as though it was an instinctive action and his presence of mind was in the response to his training. I hope he got a bonus.

Another interesting feature of the accident which I didn't get to the bottom of was that one of the passengers, also interviewed afterwards, seemed to suggest that passengers in the last carriage (ie the one about to be crushed) scrambled through the connecting door into the preceding carriage, in response to hearing the driver shouting at the signalling staff over his comms - presumably he had switched on the PA so that passengers could be warned at the same time. I hope he got two bonuses!

Martyn Ould, Praxis plc, 20 Manvers Street, BATH BA1 1PX, UK

---

### **✂ Hi-Tech Loo**

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

*Thu, 29 Mar 90 13:52:59 BST*

I just saw this on soc.culture.japan, and couldn't resist reposting it to RISKS just to see what sort of reactions it would arouse. Brian Randell

>From: lui@cbnewsm.ATT.COM (wayne.w.lui)

>Newsgroups: soc.culture.japan

>Subject: A loo full of technology  
>Date: 28 Mar 90 04:01:24 GMT [edited by PGN]

Japanese technology is plumbing new depths -- it's created the intelligent toilet. Last October, Toto Ltd., Omron Corp. and Nippon Telegraph and Telephone Corp. (NTT) jointly developed the ultimate in information technology: the fancy flusher. Makers say a trip to this toilet may save you a trip to the doctor. The intelligent diagnostic system packs the latest state-of-the-art goodies. The toilet bowl has a sensor to perform urine analyses and then zaps the data onto a display screen that shows the concentration levels of sugar, protein, urobilinogen, and blood in the urine for the occupant's viewing. Users can chart their blood pressure by sticking their left index finger into a sensor-sensitive unit on the toilet. The information then can be viewed on the second screen of the diagnostic system.

What goes in also comes out. The diagnostic system has a printer and an integrated circuit (IC) memory disk card drive that can store up to 130 examinations. The IC card can also be inserted into a compatible computer system for simple record updates. [...] NTT officials see the diagnostic system eventually having on-line communications capabilities enabling users to send information directly to hospitals or clinics.

Source: Kyodo News. Date: 24 March 1990

[This opens up all sorts of privacy issues! There is also a potential problem with a user being identified and trapped for capture. PGN]

---

## ✂ Proposed UK Authority for Risk Management

Brian Randell <Brian.Randell@newcastle.ac.uk>  
Mon, 19 Mar 90 21:59:35 BST

### MODERN HAZARDS DEMAND A 'SAFETY CULTURE'

At a time of increasing concern over both public safety and 'green issues', an Authority for Risk Management would have a vital role as Britain's main source for scientific assessment of risks. As an independent umbrella organisation, taking in such agencies as the Food Safety Directorate and the Chief Medical and Veterinary Officers, Richard North argues it would help to ensure more public confidence in official information.

The British democracy is the most mature in the world. Perhaps, accordingly, it has problems responding to a new desire in its citizens to be better informed.

An older generation accepts that the Government knows best, but this comfortable assumption has been eroded fast. Last week, a local government report described Britain's proneness to disaster as being more appropriate to a third world country.

There has been an embarrassing plethora of major disasters - Piper Alpha, the Bradford football fire, the King's Cross tube fire, the Zeebrugge ferry sinking and several others - which suggest a failure to develop a proper safety culture.

There has also been a worrying series of insidious problems.

In 1988, South West Water allowed poison into the the drinking water at Camelford; bovine spongiform encephalopathy, "mad cow disease", has invaded domestic herds; eggs and poultry have been found to be pathogenic. Groups have sprung up to complain about pesticide residues in food and veterinary product residues in farm animals.

The Authority for Risk Management, ARM, would be the formal means by which such risks - and those of nuclear power, public transport, environmental pollution, food poisoning, even global warming - are scientifically assessed, brought to public attention, rationally explained, and responses to them costed.

One of its jobs would be to develop a way of talking about the tolerability of risks; almost all of us take huge risks every day with hardly a second thought, yet get very nervous about much smaller - but involuntary - hazards.

ARM would be a creature of Parliament, and report to it. Its advice would be given in public, and ministers would have to respond in public. ARM would not be directly democratic, but would be required to hold open meetings, in the way the BBC has done in recent years. Indeed, it could develop a "roadshow" approach, taking key issues to the public, and inviting comment.

ARM's rigorously independent scientists will not be allowed to become purists. Their advice would have to be accompanied with the cost implications of new policy. The minister, public and Parliament need to know how much they are going to spend to live in a safer environment, and decide if they want to pay the price. ....

ARM would develop a culture of its own - both strictly regulatory and alert to costs. It would look a little like the Office of Technology Assessment in the USA. But OTA advises Congress, and only on specific matters drawn to its attention by elected representatives. ARM would have a stronger statutory, and innovatory, role. The creation of ARM could make Britain a world leader in the "greening" of government.

BOX: Catalogue of UK disaster and disease

The following is a list of recent key events which have encouraged discussion on whether Britain is adequately able to manage risk, whether in terms of disaster or disease.

1984 - May: 16 die in Abbeystead pumping station in Lancashire. November: Hundreds flee as fire breaks out in Oxford Circus Tube.

1985 - May: Legionnaire's disease in Staffordshire kills 30 in a month. May: Bradford City football stadium fire; 56 killed.

1986 - November: BSE identified for first time (confirming first outbreak was in 1985). November: North Sea helicopter crash; 45 dead.

1987 - March: Herald of Free Enterprise capsizes; 193 dead. October: Gale force winds lash Britain after low-key warning. November: King's Cross Fire;

31 dead.

1988 - April: Independent committee set up to investigate BSE. July: Piper Alpha explosion; 167 dead. August: Department of Health issues press release suggesting avoidance of raw eggs. October: In the year so far, 46 egg-associated outbreaks of food poisoning involving 1,000 people. December: Clapham rail disaster; 35 dead. December: Lockerbie air disaster; 270 dead. December: 26 people are reported to have died in salmonella-linked deaths in the year so far. December: Edwina Currie says most egg production is infected with salmonella. December: Government announces increased controls on egg producers.

1989 - January; M1 Boeing 737 air crash; 47 dead. February: Department of Health announces that 61 people died of listeriosis in previous year. April: Hillborough stadium crush: 95 dead. July: 2 die, 80 ill in salmonella outbreak. August: Marchioness river boat sinks; 51 dead. December: Royal Oldham Hospital salmonella outbreak; 3 dead.

1990 -January: 29,998 cases of salmonella in humans in past year, up from 27,478 in the previous year.

Brian Randell, Computing Laboratory, University of Newcastle upon Tyne, UK  
EMAIL = Brian.Randell@newcastle.ac.uk  
PHONE = +44 91 222 7923 FAX = +44 91 222 8232

---

### More on Prodigy's Updating of a User's Disks

*Eric Roskos <roskos@ida.org>  
Mon, 26 Mar 90 09:50:20*

In a recent RISKS posting, I responded to Donald B. Weschler's statement that Prodigy could update arbitrary files on the user's hard disk by saying that it appeared that Prodigy only does cache management of data in a single file, STAGE.DAT, via this method.

In response to my comment I received mail from Simson Garfinkel, who wrote the recent Christian Science Monitor article on Prodigy. He said that Prodigy's manager of software services had told him that they could indeed update other files, including .EXE files, thus avoiding the need to send out update disks.

Seeking an explanation, I asked what could be updated by this method on Prodigy's technical service bulletin board about a week ago, and also wrote to one of their technical support people asking for clarification. In response to this, Prodigy, who has always previously answered my technical questions immediately, simply ignored the question altogether. It has now been deleted from the bulletin board by Prodigy's automatic article-expiration software. Harold Goldes, the Prodigy representative who I asked about the updating, likewise did not reply.

There were several messages by users who read my posting; they all said the same thing -- that Prodigy could update .EXE files. One person said

that he had expressed concerned about the problem, but that Prodigy had replied "trust us, no one has the access needed to cause an unauthorized update." None of the posters said where they obtained their information, but all postings are screened by Prodigy's staff before appearing on the board, and Prodigy did nothing to correct these statements. Thus, I tend to believe them, since they support the statement made by the Prodigy manager.

Needless to say, this is not encouraging. I re-checked my files in the Prodigy directory this evening, and found that no file but STAGE.DAT has been updated since I installed the software nearly a year ago. I examined the contents of STAGE.DAT with a disassembler, and it does not seem to be 8086 code. It has always been my belief that STAGE.DAT contains code interpreted by the main Prodigy program, since Prodigy also runs on the Macintosh and since STAGE.DAT seems from Prodigy's previous descriptions to contain definitions of graphics screens and windows displayed while the system is operating.

If it is indeed an interpreted environment, it would be relatively easy for Prodigy to prevent unauthorized updates of anything but STAGE.DAT.

If, however, the claims are correct, the Prodigy updating mechanism would seem to be a considerable risk to Prodigy and its users, as in the case of a disgruntled employee who arranged for an "update" to occur after leaving the company, or of someone who discovered a way to circumvent Prodigy's access controls. Prodigy acknowledges the possibility of such unauthorized access by outsiders in its membership agreement: "Unauthorized access to the PRODIGY service or to restricted portions of the service is a breach of this agreement and a violation of law."

This same agreement also tries (in capital letters) to limit Prodigy's liability: "ANY LIABILITY OF PRODIGY, INCLUDING WITHOUT LIMITATION ANY LIABILITY FOR DAMAGES CAUSED OR ALLEGEDLY CAUSED BY ANY FAILURE OF PERFORMANCE, ... DELETION, ... THEFT OR DESTRUCTION OR UNAUTHORIZED ACCESS TO, ALTERATION OF, OR USE OF RECORDS ... [including] TORTIOUS BEHAVIOR ... SHALL BE STRICTLY LIMITED TO THE AMOUNT PAID BY OR ON BEHALF OF THE MEMBER TO PRODIGY FOR THE PRODIGY SERVICE IN THE PRECEDING 12 MONTHS." At current service fees, this would be a maximum of \$120 liability on the part of Prodigy for damage to a user's data.

---

### Risk-free PRODIGY

*Paul Eggert <eggert@twinsun.com>*

*Wed, 28 Mar 90 13:48:37 PST*

Here's what the PRODIGY folks say about risks in using their service. In junk mail I just got from them, the front teaser says:

A second chance to try the most exciting new  
personal computer service ever.

But you have just 7 days left to take advantage of this \_risk-free\_ offer.

Inside, there's more:

Now you can use your computer in ways  
you never did (or could) before.

But hurry, this RISK-FREE Offer expires in 7 days. [...]

And now you can try the PRODIGY service...RISK-FREE.

There's absolutely no obligation. [...]

Risk-Free OFFER TERMS: If you are not completely satisfied with the  
PRODIGY service during your first month, simply mark your first bill  
"cancel" when it comes, return it, and owe nothing. [...]

---

## **✂ April Fools Day on the net**

*"Martin Minow, ML3-5/U26 02-Apr-1990 0957" <minow@bolt.enet.dec.com>  
Mon, 2 Apr 90 06:58:26 PDT*

[an explanation for Risks redistribution problems?]

(I removed some page separators).

Network Working Group  
Request for Comments: 1149

D. Waitzman  
BBN STC

1 April 1990

A Standard for the Transmission of IP Datagrams on Avian Carriers

Status of this Memo

This memo describes an experimental method for the encapsulation of  
IP datagrams in avian carriers. This specification is primarily  
useful in Metropolitan Area Networks. This is an experimental, not  
recommended standard. Distribution of this memo is unlimited.

Overview and Rational

Avian carriers can provide high delay, low throughput, and low  
altitude service. The connection topology is limited to a single  
point-to-point path for each carrier, used with standard carriers,  
but many carriers can be used without significant interference with  
each other, outside of early spring. This is because of the 3D ether  
space available to the carriers, in contrast to the 1D ether used by  
IEEE802.3. The carriers have an intrinsic collision avoidance  
system, which increases availability. Unlike some network  
technologies, such as packet radio, communication is not limited to  
line-of-sight distance. Connection oriented service is available in  
some cities, usually based upon a central hub topology.

Frame Format

The IP datagram is printed, on a small scroll of paper, in hexadecimal, with each octet separated by whitestuff and blackstuff. The scroll of paper is wrapped around one leg of the avian carrier. A band of duct tape is used to secure the datagram's edges. The bandwidth is limited to the leg length. The MTU is variable, and paradoxically, generally increases with increased carrier age. A typical MTU is 256 milligrams. Some datagram padding may be needed.

Upon receipt, the duct tape is removed and the paper copy of the datagram is optically scanned into a electronically transmittable form.

#### Discussion

Multiple types of service can be provided with a prioritized pecking order. An additional property is built-in worm detection and eradication. Because IP only guarantees best effort delivery, loss of a carrier can be tolerated. With time, the carriers are self-regenerating. While broadcasting is not specified, storms can cause data loss. There is persistent delivery retry, until the carrier drops. Audit trails are automatically generated, and can often be found on logs and cable trays.

#### Security Considerations

Security is not generally a problem in normal operation, but special measures must be taken (such as data encryption) when avian carriers are used in a tactical environment.

#### Author's Address

David Waitzman, BBN Systems and Technologies Corporation,  
BBN Labs Division, 10 Moulton Street, Cambridge, MA 02238  
Phone: (617) 873-4323      EMail: [dwaitzman@BBN.COM](mailto:dwaitzman@BBN.COM)

---

### Automated Fast Food

*<davy@itstd.sri.com>*

*Mon, 02 Apr 90 13:41:01 PDT*

Went to the local Arby's today...

They don't have cash registers anymore. Instead, they've got touch-screens in the counter, and the customer is expected to navigate through a series of menus, touching the items he wants.

Some notes:

- The screens are IBM PS/2 color monitors, with a "micro-touch" label stuck on them

- The menus are reasonably well designed, with large squares to push, etc. Unfortunately, the screens are positioned such that the glare makes them hard to read. I expect people with bad eyesight, or who forgot their glasses, would also have problems.
- There is a "delete" option for when you screw up, or have fat fingers
- The manager thought the system was the best thing since sliced bread and pop-top beer cans. I unfortunately was there during the lunch hour, so didn't have time to engage him in conversation to find out just why he liked it so much, even in face of the obvious problems the system has.
- There is *\*no\** way to do a special order from the customer screen. When I complained about this to the manager (who was standing there making noises about how great this system was), he said "yes you can, we do it from back here". When I asked him what the point of me doing my own order was if he had to come over and adjust it for the special-ness, he just didn't seem to see the problem. Sigh.
- After you enter your stuff and press "finished order", then the person behind the counter comes up and takes your money, just like before, and they get your order for you. The whole time we were ordering, these folks were just standing around watching us. So I'm not sure how these devices are supposed to save any money/time/whatever.
- It took me about three times as long to place my order and get my food as it did before, when I'd just say "super, no sauce, fries, large coke". And I had to fill my own soft drink, too.

Another example of adding technology "because it is there", and taking a giant step backwards as a result.

Dave Curry, SRI International

---

### ✂ Re: PSU Hackers thwarted (Angela Marie Thomas, [RISKS-9.74](#))

Pete Mellor <[pm@cs.city.ac.uk](mailto:pm@cs.city.ac.uk)>

Wed, 21 Mar 90 18:23:30 PST

David C. Lawrence ([RISKS-9.75](#)) questions the validity of assigning amounts of cash to computer time and other services allegedly 'stolen' by hackers. Obviously, the sums quoted depend on what the services *\*could have\** been sold for *\*if\** the owner of the system had been running a bureau service.

Where the service is charged for only in "funny money" for departmental accounting purposes, such figures should be regarded with suspicion.

Some years ago, I was working in a department which owned an ICL 1904S running the GEORGE 3 operating system. This had an automatic accounting system which calculated charges via a complex algorithm whose parameters were defined by the system manager (so much per Kbyte of filestore space, so much per mill

second, etc.), and printed cash invoices to users every month.

Our system manager, a man not known for wasting resources, had been very successfully augmenting the departmental budget by cross-charging for bureau services provided to other departments.

One Friday afternoon, after the department had celebrated someone's imminent departure in the traditional way at the pub, he noticed that the system was clogged up by several very large core images whose size and mill consumption could only indicate mass playing of Star-Trek. He therefore ran the accounting package, traced the individuals by their account names, and duly presented them with personal bills of several hundreds of pounds each for 'computing services'.

Nobody paid up, but a few programmers got a nasty shock!

Peter Mellor, Centre for Software Reliability,  
City University, Northampton Square, London EC1V 0HB

---

### **✂ UNIX Trix**

*Paul Eggert <eggert@twinsun.com>*

*Mon, 2 Apr 90 13:09:51 PDT*

The following note is taken in its entirety from page 1 of CommUNIXque 1:1 (Second Quarter 1990), a quarterly newsletter put out by ASCAR Business Systems, Glendale, CA.

#### UNIX Trix

For those of you in the reseller business, here is a helpful tip that will save your support staff a few hours of precious time. Before you send your next machine out to an untrained client, change the permissions on /etc/passwd to 666 and make sure there is a copy somewhere on the disk. Now when they forget the root password, you can easily login as an ordinary user and correct the damage. Having a bootable tape (for larger machines) is not a bad idea either. If you need some help, give us a call.

I wonder how many UNIX machines have their security turned off this way?

---

### **✂ Three Australians indicted for computer tampering**

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

*4 Apr 90 08:37:00*

John Markoff's article in the 4 April 1990 NY Times notes the indictment and arrest of three Australians for breaking into and tampering with computers in the U.S. and Australia, after a two-year investigation. Computers included Citicorp as well as many on the Internet -- at Los Alamos National Laboratory, Harvard University, Digital Equipment Corp., Lawrence Livermore National

Laboratories, Boston University, New York University, the University of Texas and Bellcore. The three were identified as Nanshon Even-Chaim, 18; Richard Jones, 20, and David John Woodcock, 21. Jones and Even-Chaim are students and Woodcock is a computer programmer. (Handles are Phoenix, Electron and Nom.) "Dave" had previously called the NY Times.



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

**Volume 9: Issue 79**

**Monday 9 April 1990**

## Contents

- [Fixing Computer Error Cost \\$1,300 in Overtime](#)  
[Chris McDonald](#)
- [Computer problem delays Calif. Lotto payouts](#)  
[Rodney Hoffman](#)
- [Computer Glitch Cuts of Decco Sales](#)  
[Mark Adams](#)
- [Computer Animations in court testimony](#)  
[Peter Scott](#)
- [Re: Proposed UK Authority for Risk Management](#)  
[Dan Franklin](#)
- [Re: Intruders arrested](#)  
[Mike McBain via Lee Naish](#)
- [Re: More on Prodigy's Updating of a User's Disks](#)  
[Leonard Erickson](#)
- [Wonderfully mistaken letter generators](#)  
[Frank Letts](#)  
[Gary Cattarin](#)
- [Re: Automated Fast Food](#)  
[Webber](#)
- [Re: Airbus Crash: Reports from the Indian Press](#)  
[Dan Brahme](#)
- [A320 press excerpts](#)  
[Robert Dorsett](#)
- [Indian A320 crash](#)  
[Henry Spencer](#)
- [The two A320 crashes show similarities](#)  
[Martyn Thomas](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✉ Fixing Computer Error Cost \$1,300 in Overtime

*Chris McDonald ASQNC-TWS-RA <cmcdonal@wsmr-emh10.army.mil>*

*Thu, 5 Apr 90 16:25:33 MDT*

The Albuquerque Journal, Thursday, April 5, 1990, ran the subject headline. The article states that:

A combination of errors erased thousands of computer docketing entries last week at state District Court, requiring 14 clerks to work Saturday to redocket the material at an estimated cost of \$1,300 in overtime. Court Administrator Thomas Ruiz on Tuesday blamed the mishap on 'human error' and 'system error', meaning 'we allowed it to happen through the format of the computer system', he said. He added that steps have been taken to avoid a repeat occurrence. [...]

Docketing is the process by which clerks enter into the computer system summaries of all court documents filed, such as new cases, motions to dismiss, judges' orders and defendants' formal responses to lawsuits. Ruiz said every court document docketed March 27 in all four divisions--civil, criminal, domestic relations and Children's Court--was erased when an employee 'went through the wrong sequence of procedures' while intending to perform a 'backup' function. [...]

---

### **✂ Computer problem delays Calif. Lotto payouts**

*Rodney Hoffman <Hoffman.ElSegundo@Xerox.com>*

*6 Apr 90 09:41:58 PDT (Friday)*

Summarized from a story by Virginia Ellis in the Friday, March 30, 1990 'Los Angeles Times' and a small follow-up note on Saturday, March 31:

A computer failure on Thursday, March 29, forced a one day delay in payoffs for the first time in the California Lottery's four-year history. On an average day, about 550,000 people redeem winning lottery game tickets which depend on computer verification (that is, not the scratch-off game tickets, but the Lotto and Decco games).

Joanne McNabb, communications manager for the California State Lottery, said an equipment failure destroyed a small amount of the data on a computer file used to validate winning tickets. The problem was discovered when they tried to reconcile ticket sales in the validation file with the file in another computer. The lost data was reconstructed overnight from a master file that keeps duplicate information as a backup.

Just one week earlier, some Decco winners in Southern California were unable for a few hours to cash their tickets because a computer file was overloaded with winners and had to be quickly expanded.

---

### **✂ Computer Glitch Cuts off Decco Sales**

*Mark Adams <mca%medicus@uunet.UU.NET>*

*7 Apr 90 11:00:34 PST (Sat)*

[ From the San Francisco Chronicle, April 7 1990. ]

## "Computer Glitch Cuts Off Decco Sales"

Sacramento - A computer programming glitch has cut off sales of certain Decco tickets containing popular card combinations six times since the California Lottery unveiled the new game last month, officials said yesterday. The problem was discovered two weeks ago when lottery computers rejected attempts by some gamblers to buy Decco tickets containing four aces - the game's hottest selling card combination, lottery director Chon Gutierrez said.

Technicians discovered that computer programmers had built an unauthorized limit into the system that allowed only 8,000 tickets to be sold on any one card combination, Gutierrez said. The limit has been reached in six of the 28 draws since the game began March 5, preventing about 48,000 tickets from being sold - or 1 percent of total Decco plays in the half-dozen affected draws, said lottery spokeswoman Joanne McNabb.

Because California schools get at least 34 cents of every \$1 spent on the lottery, the education system has been deprived of more than \$16,300 in revenue because of the computer problem. Lottery officials are now studying ticket sale patterns to determine how much they will raise the limit. They do not want to erase the limit completely, however. State law restricts annual Decco prize payouts to 50 percent of ticket sales. If lottery officials were to remove the limit entirely, prize payouts could rise over 50 percent of ticket sales if a popular card combination were drawn several times in the game. [...]

---

## Computer Animations in court testimony

Peter Scott <PJS@grouch.JPL.NASA.GOV>

Fri, 6 Apr 90 18:46:04 PST

I've just seen a segment on ABC News Tonight which has me worried. It was about the use of computer animations in court testimony. They showed animations of plane and car crashes which used solid modelling and realistic rendering combined with animation to show what "really" happened. Nowhere in the segment did they suggest that it represented a synthesis of various points of view. One attorney asserted that he doubted he would have won his client's case without the animation of his client's ride on a roller coaster, which he claimed caused a stroke. Despite the fact that 8 million other people had ridden the coaster without ill effects, because this guy had an animation that looked like the real thing, showing g-forces on his client's head, he won his case. In another case, an animation of an accident claimed to be unavoidable was said by a juror to be convincing, because you could "really see what happened, and it was very colorful."

The RISks are obvious; going from circumstantial evidence of, say, a car crash, they animate the scene and necessarily make numerous assumptions in order to be able to produce a viewable animation. The jury is subliminally convinced that they are watching a video reenactment of the scene, and if the other side doesn't have a video of their own... the animations are likely to be viewed by jurors as direct evidence instead of indirect. The segment started

with an animation of a plane crash married with the cockpit voice recorder, and the flight recorder telemetry (?) was used as input for the animation. That's a whole lot more reliable than taking evidence from casual witnesses to a car crash and translating it to position and velocity data.

Peter Scott (pjs@grouch.jpl.nasa.gov)

---

**✉ Re: Proposed UK Authority for Risk Management**

<dan@BBN.COM>

Thu, 05 Apr 90 19:32:13 -0400

The Authority for Risk Management sounds like a good idea, but I can't help being a little put off by one comment:

> ARM's rigorously independent scientists will not be allowed to become  
> purists. Their advice would have to be accompanied with the cost  
> implications of new policy. The minister, public and Parliament need to know  
> how much they are going to spend to live in a safer environment, and decide  
> if they want to pay the price. ....

This paragraph presents risk management as though it must necessarily cost money, and the only issue is to decide whether to pay the price. But it should be obvious to any government, particularly one that runs a national health service, that reducing a risk can SAVE it money! If fewer people are poisoned or hurt, health costs go down. Governments lacking a national health service or other direct connection to health costs should consider the savings to society as a whole (that's theoretically why government does things, after all).

Admittedly, once you start doing this, you often end up trying to decide just how valuable it is to save or prolong a given life. Not a great situation, but "not to decide is to decide" anyway.

Dan Franklin

---

**✉ Re: Intruders arrested**

Lee Naish <lee@munmurra.cs.mu.OZ.AU>

6 Apr 90 03:17:32 GMT

In article <862@sirius.ucs.adelaide.edu.au>, simon@ucs.Adelaide.EDU.AU (Simon Hackett) writes:

> There is some (quite) recently enacted state law in SA which makes it  
> illegal to access a "restricted access" computer system without  
> authorization. Doesn't matter whether you do anything, this is simply  
> making it illegal to log into any system for which you require a  
> password, where you ain't a person who should be using it. Restricted  
> access is defined in the enactment of the law in a form of words which  
> means the above.  
>

- > There is a second offence defined, which equates to unauthorized
- > modification of information in a system.
- >
- > Both offences carry 2 years/\$2000 fine as maximum penalties.

In a related vein, here is an item from the Melbourne 'Age' 3/4/90

'Man fined \$750 for computer trespass', by Geoff Winestock

A man who copied a confidential set of programs from the computer company where he worked became the first person convicted under a new computer trespass law yesterday. Alexander Belkin, 31, of Latona Avenue, Knoxfield, was fined \$750 in Prahran Magistrate's Court for gaining access to a computer without lawful authority. He was also fined \$250 for unlawful possession of a library book. On 1 April 1989, Belkin, who worked for GNA Computing Pty Ltd, copied some business record systems without specific authorisation from his employer.

Mr David Bamber, for Belkin, said the computer trespass law should be viewed as analogous to ordinary trespass, for which it was necessary not just to prove an incident had occurred but that it was done with criminal intent. Otherwise, he said, the offence of computer trespass could extend to thousands of schoolchildren operating computers without permission or employees going about their business.

But the magistrate, Mrs Heather Spooner, said the facts of the case were clearly covered by the legislation. The law applied not only to offences where there was criminal intent, such as computer hacking and theft, but also to regular users, such as employees. Mrs Spooner said the law was a response to calls from the computer industry and police to stop the harm caused by mere access or "intellectual voyeurism". Prosecution was necessary in a case such as this, which involved computer programs of great value. She said the application of the law would require considerable common sense. Schoolchildren operating computers should not be in jeopardy. Mrs Spooner said that Belkin's evidence on matters such as the workstations he was authorised to use and the copies he was allowed to make on floppy disks had been inconsistent with that of his employer. She concluded that he had not been honest.

Belkin would bear the cost of his mistake for the rest of his life, especially in his standing in the industry, and she had taken this into account in sentencing him.

Mike McBain, Avid Systems Pty Ltd, St Kilda, Australia 3182

---

### **Re: More on Prodigy's Updating of a User's Disks**

*Leonard Erickson <leonard@nosun.West.Sun.COM>*

*Fri, 6 Apr 90 23:33:43 PDT*

CompuServe has had the ability to do this for at least 9 years. Their L-Protocol was \*specificly\* designed so a user could enter a short BASIC program which would call in, download \*and execute\* a terminal program.

The B-protocol description includes this feature *\*explicitly\** in the protocol description, along with such features as "disable keyboard" and disable video updates". I *\*think\** the older A protocol also had these features.

All of these CIS protocols include a whoami string that sends an identifier string that identifies the machine type, software version, and protocols supported in response to a remote query. This response is invisible to the user.

I know that some people used programs like CIS's VIDTEX for their *\*only\** terminal program. I once considered having a BBS check for such people and do something to their machine... it would be rather easy.

This is not a new risk, but it is more widespread than some think.

--

Leonard Erickson     ...!tekrnix!reed!percival!bucket!leonard  
CIS: [70465,203]

"I'm all in favor of keeping dangerous weapons out of the hands of fools.  
Let's start with typewriters." -- Solomon Short

---

### **✶ Wonderfully mistaken letter generators**

<letts@ficc.UUCP>  
Thu Apr 5 22:49:08 1990

Several posts in [RISKS-9.78](#) reminded me of a humorous incident down here in Sugar Land, Texas, in the early 1970's ('73, I think). A letter similar to the below arrived one day in the office of the Eldridge Road Church of Christ:

Congratulations, Mr. Christ! Our computer has selected you as only one of a few to receive a set of lucky numbers in our (who rememebrs) sweepstakes!

Yes, Mr. Christ, you and the entire Christ family may be the ones to enjoy a full expense paid trip to Hawaii, or a new Cadillac!

Be sure to return your sweepstake numbers today and qualify for the early-bird bonus! And while you are at it, place your NO obligation order for our latest publication [some book named here], something that the Christ household certainly should not be without!

That still cracks me up when I am reminded of it.

Frank Letts, Sugar Land, Texas

---

### **✶ Wonderfully mistaken letter generators**

<Gary\_Cattarin@DG\_SUPPORT.MCEO.DG.COM>

*Fri, 6 Apr 90 13:35:08 edt*

CEO summary:

The item from Yuri Rubinsky in [RISKS 9.78](#) concerning the letter he received indicating that the letter he desired was backordered reminded me of a wonderful abuse of software I received several years ago. I was still a "minor" as they say, or "underage", and my grandmother had set up a "custodial account" money market. These accounts were addressed as: Granny Smith, Cust

Joe Underage UGMA/NY

Or, in English:

---

### **✂ Re: Automated Fast Food**

*<webber@psych.toronto.edu>*

*Fri, 6 Apr 90 17:13:56 EST*

In [RISKS Digest 9.78](#), Dave Curry (davy@itstd.sri.com) wrote about automation at his local Arby's. [...] It seems to me that what he's actually seen is the first phase of implementation and testing of this new system, and that the management of Arby's is sensibly keeping the old system in place. If this touch-screen stuff can be made to work properly and is accepted, he will probably not see staff members hanging around doing nothing for long: Arby's outlets will reduce staff to the minimum required to cook, deliver hot food, clean, and take money.

I have read that the largest overhead for the operation of a fast-food restaurant (where they serve food which makes you feel that you might as well fast) is the cost of personnel. If this is true, then with increased automation profits have the potential to rise a great deal. Of course, there's a risk to the management and to other members of US society in this kind of change: not only may Arby's lose customers, due to decreased service quality, but some low-income families will have their incomes reduced even further as the pool of service jobs they've depended on dries up.

---

### **✂ Re: Airbus Crash: Reports from the Indian Press**

*Dan Brahme <brahme@vlsic2.ti.com>*

*23 Mar 90 23:03:57 GMT*

henry@zoo.toronto.edu writes:

>Aviation Week reports that India refused European airworthiness authorities'  
>request to participate, and also refused information requests from them and  
>from Airbus Industrie. Henry Spencer at U of Toronto Zoology

Not really. The reason to exclude the Europeans from the investigation is to prevent doctoring or tampering with evidence. It is very surprising that the French have started talking about carelessness of the pilot. If they do not have access to the investigating teams report how can they talk about carelessness of the pilots. I fly all the time in North America and quiet often in Europe and India. In fact the quality of Indian pilots is very good and the average may in fact be better than the europeans judging by smoothness of the

landings.

The A320 has a lot of software in it. Anybody who has any knowledge of large software systems knows that it is often the source of many problems. A look at how many times the space shuttle launch had to be postponed due to some software problem should shed some light.

Considering that, if there is a (or many) technical problem and Indian Airlines continues to fly the plane and there is another accident many more lives will be lost. On the other hand, if all the planes are grounded and later on it is found that there is no problem with the plane, then the cost to AIRBUS is at most a possible loss of sales for a short period. If this results in loss of some jobs, I am sure the engineers can find another job or live on their savings or welfare. Considering the alternative (1) few frenchmen losing jobs to (2) several indians dying, I don't think there is anything wrong with grounding. In fact if the airline had not grounded the rest of the planes I would have been one of the first to protest.

The behavior of Airbus displays complete lack of concern for human life and shows that they care only for profits at all costs. It also shows that they are willing to introduce UNSUBSTANTIATED reports in an attempt to cover their ass.

It is interesting to note that not a single message of condolence was sent by the airbus president to the families of those who died in the accident. If such an accident took place in the US and AIRBUS behaved the way it did it would lose credibility with the american public and it would suffer severe financial loss due to lawsuits filed in US courts.

Dhananjay Brahme

---

### **A320 press excerpts**

*Robert Dorsett <rd@walt.cc.utexas.edu>  
Fri, 30 Mar 90 21:44:34 -0600*

The following are from the February 21st and 28th issues of FLIGHT INTERNATIONAL, and actually appear to be somewhat authoritative. They clarify various information/misinformation which has appeared on RISKS and sci.aeronautics over the past month. [I've interspersed my own comments (brackets). Take those with a grain of salt. :-)]

\* The airfield had no ILS approach. VOR/DME, NDB only. Runway length was 10850'. Field elevation 2914' No significant terrain nearby. Visibility was unlimited at the time. The crash occurred at 1300 local time [1PM].

\* The approach was being made manually. There were no reported emergency communications between tower and aircraft. The landing gear was down.

\* Airplane collided with the ground approx. 500 meters from threshold, in a golf course, bounced, and came to rest 100 meters from the end of the runway. FLIGHT characterizes the initial impact as "soft." [ note: bounces are generally the result of the aircraft having too much velocity, and not,



## **✂ Indian A320 crash**

<henry@zoo.toronto.edu>

Mon, 2 Apr 90 00:06:35 EDT

One of the bigger problems in assessing the A320 is that almost everyone has vested interests to protect. Most European aircraft manufacturers are involved in building it, so they (and their governments) want it to be a commercial success. Their US competitors (and their government) would prefer it to be a commercial failure. Pilots' unions often oppose it because it is a 2-man-crew aircraft replacing 3-man-crew planes. And so on. The relevance of this to the Indian crash is that India, lacking its own facilities for reading modern crash recorders, sent the A320's recorder to Canada for analysis. They chose Canada specifically because it has no vested interest in the A320!

Incidentally, the latest word in Flight International (21 March issue) is that informal reports -- admittedly thirdhand -- claim the approach was being flown at an excessively low speed, 106 knots as against a recommended speed of about 130 at that point, just before the crash.

Henry Spencer at U of Toronto Zoology  
uunet!attcan!utzoo!henry henry@zoo.toronto.edu

---

## **✂ A320 crashes show similarities**

Martyn Thomas <mct@praxis.UUCP>

Mon, 2 Apr 90 12:48:45 BST

Flight International, 4-10 April 1990, page 6:

"Cockpit voice recorder (CVR) and digital flight data recorder (DFDR) information from the Bangalore accident made available to A320 operators indicates that the cause was remarkably similar to that which the Investigation Commission found for the A320 accident at Habsheim, France, in June 1988. The CVR makes it clear that the right-hand-seat pilot intentionally selected "idle" on the autothrottle as the aircraft descended through 500ft (150m) on Bangalore final approach. This increased the aircraft's rate of descent as intended, but reapplication of power came too late to arrest the vertical speed and prevent the aircraft hitting the ground short of the runway. According to the DFDR, full power was tripped in automatically by the Alpha Floor protection mode as the aircraft passed 135 ft. This implies that the handling pilot had selected maximum angle of attack to arrest vertical speed, but at low indicated airspeed (IAS). The IAE V2500 engines were not fast enough spooling up to full power to provide the additional IAS needed to generate the increased wing load factor to arrest the rate of descent. At Habsheim, the aircrew also selected power-up from idle too late and, as a result, failed to clear trees at the airfield edge."

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK.  
Tel: +44-225-444700. Email: ...!uunet!mcvax!ukc!praxis!mct



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

**Volume 9: Issue 80**

**Friday 13 April 1990**

## Contents

- [Risks of Daylight Savings Time](#)  
[Chuck Weinstock](#)
- [Authentication via User-Defined Fields](#)  
[Jim Kimble](#)
- [Rites of consumption](#)  
[Phil Agre](#)
- [Franklin Resources Computer Glitch](#)  
[John Murray](#)
- [Risks of computerized publishing](#)  
[Henry Spencer](#)
- [Re: Computer generated letters](#)  
[Benjamin Ellsworth](#)  
[Nathaniel Borenstein](#)
- [Software: A320 vs. shuttle](#)  
[Michael](#)
- [The C3 legacy, Part 5: Subsystem I](#)  
[Les Earnest](#)
- [COMPASS 90 program and registration information](#)  
[John Cherniavsky](#)
- [Info on RISKS \(comp.risks\)](#)

---

### Risks of Daylight Savings Time

*Chuck Weinstock <weinstoc@SEI.CMU.EDU>*  
*Mon, 09 Apr 90 16:34:47 EDT*

With the time change a week ago, I personally experienced the results of a programming error. On Saturday, March 31, some friends and I left Chicago on the Amtrak train Southwest Chief bound for Flagstaff, AZ. Because of the time change that occurred that night, the train was automatically an hour late at 3am on the 1st. This meant that we would arrive in Flagstaff at 10:24pm Sunday instead of the 9:24pm scheduled. However, by Albuquerque due to some excellent train handling by the Santa Fe Railroad, the train had made up most of that

hour, and by Winslow, the first stop in Arizona, we were on time.

Unfortunately the Amtrak ticket computer had not been programmed correctly to deal with daylight savings time in Arizona (there isn't any...it retains Mountain Standard Time == Pacific Daylight Time), and the incorrect train departure time had been printed on the tickets. The conductor decided we couldn't leave Winslow until the time on the tickets, so we sat in the station for an hour and eventually arrived in Flagstaff an hour late.

Chuck Weinstock

---

### **✶ Authentication via User-Defined Fields**

*The Programmer Guy <jkimble@nostromo.austin.ibm.com>  
Mon, 9 Apr 90 15:43:01 CDT*

I was picking up a prescription at my local pharmacy when I was told by the clerk that the order had not yet been phoned in by the doctor. I was asked to wait for a few minutes while the clerk rifled through a stack of FAXed prescriptions.

After the clerk found the FAX from my doctor's office and passed it on to the pharmacist, I began thinking how easy it would be to forge a prescription by using your favorite desktop publishing software, a scanner, and a PC-FAX board. This might have taken a little skill and a lot of ingenuity a few years ago, but as extremely easy-to-use software proliferates into the general public, this task becomes almost trivial.

I asked the clerk how they went about verifying that the FAX transmissions were legitimate. She said the Sending FAX transmits the name of the doctor's office and its phone number; the clerks simply ensures that the phone number listed is correct. The obvious flaw in this system is that the FAX machine itself does NO VERIFICATION of your name or phone number -- you simply "roll your own" banner as you see fit! The hopper holding the received documents was sitting in plain sight so obtaining a "legitimate" banner wouldn't be at all difficult.

I point this out as an example that the only thing worse than \*no\* verification of authenticity, is \*assumed\* authenticity.

--Jim Kimble, TCP/IP Development, IBM Austin, TX

---

### **✶ Rites of consumption**

*"Phil Agre" <agre@gargoyle.uchicago.edu>  
Mon, 9 Apr 90 17:35:33 199*

The articles about automation in fast food restaurants brought to mind a recent article in the New York Times about the McDonald's in Moscow. It seems that the Russians did not yet have the skills necessary to eat at McDonald's. In particular, though they all have extensive experience at waiting in line, they

were accustomed to lines parallel to the counter, not orthogonal to it. And they were entirely unaccustomed to the precise, stylized form of dialogue that is involved in purchasing a meal at such a restaurant. The exuberant managers of the restaurant had taken this as a kind of challenge, it seems, and declared their intention to "McDonaldsize" the Russians. For the managers of McDonald's, this wasn't just a matter of helping the poor Russians learn to order a hamburger, nor was it simply a matter of running an efficient restaurant. It was symbolic, both for the people who own McDonald's and for the New York Times -- the perspectives of the two of them were quite indistinguishable throughout -- of the larger process of 'converting' the Russians to a capitalist way of life. It was explicit in their explanations of this process that living in a capitalist social and economic system is a \*skill\*, something located not nearly so much in the mind as in the body, in a cultivated habituation to the various forms and interfaces of efficient consumption. It would seem that these Russians are getting their remedial lessons just in time, given that the process of buying fast food is about to become even more of a skill. The touch screens will be confusing at first, given that everyone has been so reliant upon the small space of 'slop' in the human contact -- minimal, to be sure, but real -- between consumer and counter attendant. But soon we will all get used to it, and the skill of sorting one's desires into the combinatorial space of a touch-screen menu will become part of each new citizen's socialization, another technological boundary joining our own bodies to the rational machinery of a system without a face or a meaning beyond the pure excitation of standardized desires.

Phil Agre, University of Chicago

---

### ✂ Franklin Resources Computer Glitch

John Murray <johnm@uts.amdahl.com>

9 Apr 90 21:22:19 GMT

Franklin Resources of San Mateo CA was criticized recently in the San Francisco Chronicle over its sales commission policy. The company runs a family of "loaded" mutual funds, meaning that customers pay an up-front commission charge to invest. The criticism related to how Franklin charges an additional, hidden commission on those dividends which are reinvested in the fund, rather than paid out in cash. It turns out that the fine print contains a provision which allows an investor to avoid this hidden commission by paying a minimum annual fee of \$50. However, Franklin doesn't promote this discount feature.

According to the Chronicle (April 7 1990), the company will soon kill the special arrangement. Chuck Johnson, VP of corporate development, says "It was never a deliberate policy, it was a data processing snafu which we ignored for a while. But an increasing number of brokers caught on, and it's reached the point where we have to address it."

Some points to ponder:

- 1) A prospectus is the legal document on which an investor is supposed to make financial decisions. But what's to stop Franklin, or anyone else, from arbitrarily ignoring ANY of its provisions, and blame a

data processing snafu?

2) What sort of 'snafu' could possibly cause a variety of prospectuses to contain a complete description of a non-existent feature? A text processing error seems most likely, but that doesn't say much for Franklin's proof-readers.

Mr. Johnson makes Franklin seem particularly sleazy. The company waited until "an increasing number" of brokers (not just one or two) drew attention to the error, or "caught on" as he puts it. Then, instead of sending out correction notices, the company just "ignored it for a while".

In any case, it seems that Franklin will no longer let you pay them to avoid having to pay them for getting what you originally paid them to do up-front in the first place!

- John Murray, Amdahl Corp. (My own opinions, etc.)

---

### ✂ Risks of computerized publishing

<henry@zoo.toronto.edu>

Thu, 12 Apr 90 23:20:19 EDT

The April issue of Locus, the major trade magazine of science fiction and fantasy writing and publishing, contains an interesting news item. Some excerpts:

\_The\_Fall\_of\_Hyperion\_, the new book by Dan Simmons, appeared with a critical page missing. All 20,000 copies of the hardcover and trade editions were shipped before bookseller and Locus reviewer Tom Whitmore called Bantam/Doubleday/Dell to point out that page 305 is missing, and page 306 appears twice. Their initial statement is not printable...

The page was correct in the advance galleys... The mistake was in the film shooting at the printer. Now that publishers and printers are computerized, there seem to be more mistakes, not less. Last year, Tor's edition of \_Angel\_Station\_ by Walter Jon Williams had several sections turned into gibberish by a computer glitch. Again, the checked galleys were correct...

The piece goes on to mention that such problems, of course, are not new. There have been some major disasters -- entire chapters or crucial scenes omitted -- even in pre-computer days.

Henry Spencer at U of Toronto Zoology      uunet!attcan!utzoo!henry

---

### ✂ Re: Computer generated letters

Benjamin Ellsworth <ben@hpcvlx.cv.hp.com>

Mon, 9 Apr 90 17:25:06 pdt

> [great story about a erroneous computer generated letter and bogus  
> signature]... [These tales continue to come out of the woodwork. Please  
> don't take this as a challenge to submit still more of them. Thanks.  
> PGN!]

Yes, but in the interest of good science (and having a good laugh ;-)) we should definitely collect an archive of as many as possible. You never know when such data will be needed by a someone doing a "study." ;-)

This is a call for such stories. If you have a story, please send it to ben@cv.hp.com. If the incident happened to you, make your subject "Letter story, first-hand." If you just heard the story, the subject should be "Letter story, hearsay." Mailings using other subject lines are not guaranteed to make it into the archive.

Once the mailing slows down a little, I'll find away to make the archive generally available.

Benjamin Ellsworth | ben@cv.hp.com

---

### **✶ Re: Wonderfully mistaken letter generators**

Nathaniel Borenstein <nsb@thumper.bellcore.com>

Tue, 10 Apr 90 00:15:58 -0400 (EDT)

My mother-in-law is the President of a small synagogue, Congregation Beth El in Potsdam, NY. She frequently receives some very amusing examples of this form, most notably ones that conclude from the "Beth" that the recipient is female, e.g.:

Dear Miss. El,

Dear Beth,

And of course, they make frequent references to "the El family" which is particularly amusing when you realize that "El" in this context means nothing less than God Himself (Beth El is Hebrew for "House of God").

In a related matter, one of my relatives, whose last name is Glasser, decided to throw away \$17 on the "Glasser family newsletter". This turned out to be a 20 page Macintosh-generated newsletter that was obviously completely generic -- globally replacing "Glasser" with "Smith" would have yielded an equally reasonable Smith family newsletter. Anybody know how much money such companies manage to make by selling such dubious computer-personalized products?

---

### **✶ Software: A320 vs. shuttle (RISKS-9.79)**

<bigm@batserver.cs.uq.oz.au>

Wed, 11 Apr 90 10:36:53 EST

brahme@vlsic2.ti.com (Dan Brahme) writes [...]

>A look at how many times the space shuttle launch had to be postponed  
>due to some software problem should shed some light.

I don't think you can validly compare the two systems, the shuttle software was a generation or more of technology behind that of airbus. I remember reading an article in communications of the ACM about the shuttle software (1982 I think), and in many ways it was a disaster waiting to happen. The method of mutual exclusion used in the shuttle was called "alibies" and involved proving that at the instant your process wanted to access a variable, no other process would. This was dubious for a few processes, but when the system complexity increased trying to calculate this  $n^2$  problem for 10's to 100's of processes was ridiculous. One of the reasons for delay was each time someone wanted to change a process, they had to recalculate all its alibis.

When one of the first flights was delayed due to weather, and the crew went back to base to practice more in the simulator. (Real shuttle software/hardware attached to a enviroment simulator.) They ran a senario called "Trans-Atlantic Abort" in which something happens to thrust so that they are too high to return to base, and too low to go into orbit. The idea was to glide to Spain. In the middle of this, all CRTs went into an error mode indicating they had not recieved any updated info from the computers in 5 seconds, and that there data was invalid. The astronauts were understandably shaken, and the software enginiers traced the problem to a bad "goto" into the middle of code without reinitialising the data.

The shuttle software was written in a goto orientated sequential language on redundant IBM computers of the same design. The A320 has 3 or 4 separate computers with CPU's from different manufactures each running software from different companies written with different compilers for high level languages that include process management and security. Goto's are forbidden in the design.

This makes it likely that the problem (if any) in the airbus software is in the problem specification/design rather than the implementation.

I have been appalled at Airbus' behaviour regarding the A320. It is not unlikely that there are some software errors, but until now Airbus has had an excellent reputation for installing good saftey features not available on other aircraft (e.g. completely fire retardent cabin materials with non toxic fumes years ahead of other manufacturers). It seems silly to risk that reputation by not being as open as possible.

Michael

---

### ✶ The C3 legacy, Part 5: Subsystem I

Les Earnest <LES@SAIL.Stanford.EDU>

11 Apr 90 1635 PDT

(Continuing from [RISKS 9.74](#))

Of the dozens of command and control system development projects that were initiated by the U.S. Air Force in the early 1960s, none appeared to perform its functions as well as the manual system that preceded it. I expect that someone will be willing to argue that at least one such system worked, but I suggest that any such claims not be accepted uncritically.

All of the parties involved in the development of C3 systems knew that their economic or power-acquisition success was tied to the popular belief that the use of computers would substantially improve military command functions. The Defense Department management and the U.S. Congress must bear much of the responsibility for the recurring fiascos because they consistently failed to insist on setting rational goals. Goals should have been specified in terms of information quality or response time for planning and executing a given set of tasks. The performance of these systems should have been predicted in the planning phase and measured after they were built so as to determine whether the project was worthwhile.

Instead, the implicit goal became "to automate command and control," which meant that these systems always "succeeded," even though they didn't work. Despite a solid record of failure in C3 development, I know of just one such project that was cancelled in the development phase. That was Subsystem I, which was intended to automate photo-interpretation and was developed for the Air Force by Bunker Ramo, as I recall.

The "I" in the name of this project supposedly stood for "Intelligence" or "Interpretation." This cryptic name was apparently chosen to meet the needs of the prospective users in the intelligence community, who liked to pretend that nobody knew what they were doing. This pretense occasionally led to odd conduct, such as when they assigned code names to various devices and tried to keep them secret from outsiders. For example, a secret name was assigned to one of the early U.S. spy satellites -- as I recall it was Samos -- but when that name somehow showed up in the popular press they tried to pretend that no such thing existed. In support of this claim, everyone in the intelligence community was directed to stop using that name immediately.

When I attended a meeting in the Pentagon a few days after this decree and mentioned the forbidden word, the person operating the tape recorder immediately said "Wait while I back up the tape to record over that!" This was a classified discussion, so there was no issue of public disclosure involved, just the belief that there should be no record of the newly contaminated name.

Sometime in the 1981-82 period, the Air Force decided to terminate the development of Subsystem I. A group of about 30 people from various parts of the defense establishment, including me, was invited to visit the facility in suburban Los Angeles where the work was going on to see if any of it could be used in other C3 systems. We were given a two day briefing on the system and its components, the principal one being a multiprocessor computer.

The conceptual design of this Polymorphic Computer, as they called it, was attributed to Sy Ramo, who had earlier helped lead Hughes Aircraft and Ramo-Wooldridge (later called TRW) to fame and fortune. The architecture of

this new machine was an interesting bad idea. The basic idea was to use many small computers instead of one big one, so that the system could be scaled to meet various needs simply by adjusting the number of processors. The problem was that these units were rather loosely coupled and each computer had a ridiculously small memory -- just 1K words. Each processor could also sequentially access a 1K buffer. Consequently it was very awkward to program and had extremely poor performance.

I sought out the Subsystem I program manager while I was there and asked if our group was the only one being offered this "free system." He said that we were just one of a number of groups that were being flown in over several months time. When I asked how much they were spending on trying to give it away, he said about \$9 million (which would be equivalent to about \$38 million today). The Air Force Systems Command seemed to be trying desperately to make this program end up as a "success" no matter how much it cost. When I asked why the program was being cancelled, I got a very vague answer.

I did not recommend that my group acquire any of that equipment and as far as I know nobody else did. The question of why Subsystem I was cancelled remained unresolved as far as I was concerned. It is conceivable that it was because they figured out that it wasn't going to work, but neither did the other C3 systems, so the reason must have been deeper (or shallower, depending on your perspective). My guess is that they got into some kind of political trouble, but I will probably never know.

(Next part: the Foggy Bottom Pickle Factory)

-Les Earnest (Les@Sail.Stanford.edu)

---

## **COMPASS '90 program and registration information**

*John Cherniavsky <jcc@cs.UMD.EDU>*

*Thu, 5 Apr 90 10:58:07 -0400*

COMPASS '90 Monday June 25  
PRE-CONFERENCE TUTORIALS

0800 Registration; Coffee  
0900 Software Safety by Archibald McKinlay of McDonnell-Douglas Corporation  
  
1300 Software Verification and Validation for High Risk Applications  
by Janet R. Dunham and Linda Lauterbach of Research Triangle Institute  
1700 Close of tutorials

COMPASS '90 PROGRAM: Tuesday June 26

0800 Registration; Coffee  
0900 Opening, General Chair, Dolores R. Wallace,  
National Institute of Standards and Technology  
  
0915 Honorary Chair Address, Honorable Mike Parker,  
U.S. House of Representatives

0930 Keynote Address, "Safety in Numbers?" Air Marshal M J D Brown,  
RAF, Director General of Strategic Electronic Systems,  
UK Ministry of Defence

1030 Program Chair, H. O. Lubbes, Naval Research Laboratory

1100 Break

1130 Systems Engineering: The Forgotten Discipline, Dario De Angelis,  
Logicon

Verification and Validation: A Systems Engineering Discipline  
for Producing Quality Software Systems, Roger Fujii, Logicon

1300 Lunch

1400 A Vital Digital Control System with a Calculable Probability of an  
Unsafe Failure, David Rutherford, Rail Transportation Systems, Inc.

1430 Using Symbolic Execution to Aid Automatic Test Data Generation,  
A. Jeff Offut, E. Jason Seaman, Clemson University

1500 A Case Study: Production Problems in an Application Running on the  
Prodigy Service, Marnie L. Hutcheson, Prodigy Services Company

1530 Break

1600 Fast Static Analysis of Real-time Rule-Based Systems to  
Verify Their Fixed Point Convergence, Albert Mo Kim Cheng,  
Chih-Kan Wang, University of Texas at Austin

1630 Real-Time Software Failure Characteristics, Janet R. Dunham,  
Research Triangle Institute and George Finelli,  
NASA Langley Research Center

1700 Uncovering Redundancy, Rule-Inconsistency and Conflict in  
Knowledge Bases via Deduction, James McGuire, Lockheed AI Center

1900 Banquet; On Quality, W. Earl Boebert, Secure Computing  
Technology Corporation

COMPASS '90 PROGRAM: WEDNESDAY June 27

0830 Registration; Coffee

0900 Mathematics for Digital Systems Engineering, Donald Good,  
Computational Logic, Inc.

1000 The Rigorous Specification and Verification of the Safety Aspects of a  
Real-time System, Derek P. Mannering, Rex, Thompson & Partners, LTD

1030 An Analysis of Ordnance System Software Using the MALPAS Tools,  
Ken Hayman, Department of Defence, Australia

1100 Break

1130 Proving Proof Rules: A Proof System for Concurrent Programs,  
David Goldschlag, Computational Logic, Inc.

1200 A Formal Approach to Railway Signalling, W. J. Cullyer and W. Wong,  
University of Warwick

1230 A Structured Approach to Code Correspondence Analysis, J.W. Freeman  
and R. B. Neely, Ford Aerospace Corporation

1300 Lunch

1400 Maintaining Abstractions with Verification, William D. Young and  
Warren A. Hunt, Jr., Computational Logic, Inc.

1430 Using CSP to Develop Trustworthy Hardware, Andrew P. Moore,  
Naval Research Laboratory

1500 Break

1530 Trusted Computer System Standards, Chuck Pfleeger, Trusted  
Information Systems

1630 Panel: Are Trusted Computer System Standards Useful for the  
Development of Systems Whose Criticality Is Other Than Security?  
Chair, H. O. Lubbes, Naval Research Laboratory

COMPASS '90 PROGRAM: THURSDAY June 28

0830 Registration; Coffee

0900 Rationale for the Development of the UK Defence Standards for  
Safety-Critical Software, Air Marshal M J Brown, RAF, Director  
General of Strategic Electronic Systems, UK Ministry of Defence

1000 Safety-related Programmable Electronic Systems: Guidelines and  
Standards, R. Bell, Health and Safety Executive, UK

1030 DRIVE-ing Standards - A Safety Critical Matter, T. F. Buckley,  
P. H. Jesty, K. Hopley, and M. West, University of Leeds

1100 Break

1130 Panel: Should Government Regulate Medical Software?  
Chair: Diane Jackinowski, Varian Associates

1230 The Computer-Related Risk of the Year: Distributed Control,  
Peter Neumann, SRI International

1300 Lunch

1400 SAFETYNET 89, Digby Dyke, Charter Technologies, LTD

1430 Product Liability in the UK - Issues for Developers of Safety-  
Critical Software" - Ranald Robertson, Stephenson Harwood Solicitors

1530 Break

1600 Panel: Are Certification and Accreditation Useful Concepts for Safety  
Critical Systems? Chair, H. O. Lubbes, Naval Research Laboratory

1700 Verifiable Microprocessors: Architectures and Verification  
Techniques, John Kershaw, Royal Signal and Radar Establishment  
and John Wise, Charter Technologies, LTD

FOR REGISTRATION INFORMATION, PLEASE CONTACT

Dolores Wallace wallace@swe.ncsl.nist.gov 301-975-3340

SPONSORS: IEEE AESS, IEEE NCAC, in Cooperation With: ACM SIGSOFT. Co-sponsors:  
Advanced Ordnance Technology Incorporated, Charter Tehcnologies, Ltd.,  
Computational Logic, Incorporated, Computer Sciences Corporation, Georgetown  
University, Logicon, Incorporated, National Institute of Standards and

Technology, Naval Research Laboratory, Naval Surface Warfare Center, Research Triangle Institute, Tri-Service Software System Safety Working Group, Trusted Information Systems



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 9: Issue 81

Wednesday 18 April 1990

## Contents

- [RISKS, SENDMAIL, and YOU!](#)  
[PGN](#)
- [London Tube train leaves ... without its driver](#)  
[Stephen Page](#)
- [Shuttle roll incident on January '90 mission](#)  
[Henry Spencer](#)
- [Software failures on Boeing 747-400?](#)  
[Trevor Warwick](#)
- [False 1099 forms](#)  
[Phil R. Karn](#)
- [Re: Risks \[9.080\] of Daylight Savings Time](#)  
[Thomas Zmudzinski](#)  
[Chuck Weinstock](#)
- [Comment on UK Software Standards](#)  
[Richard Morton](#)
- [Automates Fast Food](#)  
[David Bank](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✉ RISKS, SENDMAIL, and YOU!

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

Tue, 17 Apr 1990 10:11:36 PDT

If you are wondering why you have not seen many issues lately,

1. I was travelling for almost two weeks, and have been utterly swamped trying to recover since I returned.
2. The SENDMAIL multiple-mailing problem has continued to bug us, hitting a DIFFERENT one of the six main SUBLISTS on the average of EVERY OTHER ISSUE. Thus, to try to minimize your agony and my annoyance, I have favored fewer but larger issues. (Yes, that could be a part of the problem, too. However, in general, it appears that the trouble has

usually been due to the combination of noncompliant remote hosts and nameserver problems. I've also had to drop a few addresses that were hanging in a name server loop!

3. At long last, we are about to install a new version of SENDMAIL for which claims are made that it improves some things, but also continues to handle awkward addresses properly and does some of the other things we need, preventing us from backing off to an earlier warhorse version. Perhaps some of the old problems will now go away, although I shudder at the thought that we may now have to discover some new problems. At any rate, please bear with us.

4. We still have a lot of .ARPA addresses, even though the ARPANET is essentially kaput. I trust those of you will provide updated addresses before it is too late. Let's not wait until the address grace period expires.

Thanks for your patience. PGN

---

### ✉ [London] Tube train leaves ... without its driver

Stephen Page <sdpage@prg.oxford.ac.uk>

Mon, 16 Apr 90 14:39:04 bst

[an article by Dick Murray in the [London] Evening Standard under the above title, 12 April 1990.]

The Runaway train went down the track -- leaving an embarrassed Victoria Line Tube driver standing behind on the platform. He had broken a golden rule and left the cab of his fully-automated train to check a door which had failed to close properly. When the door did shut an electrical circuit was completed and the train, with 20 passengers on board, moved off before the driver had time to rush back to the controls.

A London Underground spokesman, stressing that there was no danger to any of the passengers, said today: 'He did not turn off the automatic-mode switch before leaving the cab.' The driver, whom Underground chiefs refused to name, then had to wait on the platform for six minutes before he could get on the Tube [train] behind to catch up with his own train.

Passengers did not know what had happened, except there was nobody to open the doors at Pimlico until the inspector let them out.

Now a full-scale inquiry into the incident, at 11.20pm on Tuesday, has been launched by London Underground and the driver could face a disciplinary charge.

[ Readers who have visited London may sympathise with my own theory, which is that the train was so astonished to be less than 400% full that it bolted. - S ]

[Yes, the normal situation is "tuBe or not tuBe, that is congestion."  
But he was certainly optimistic to think that he could CATCH UP with

his train, since the automatic controls clearly are designed to prevent that. A better strategy would have been to call ahead. But I presume that the supervisor commandeered a substitute driver anyway. Actually, the train is not COMPLETELY automatic; the opening and closing of doors is controlled manually. But perhaps there is an interlock that keeps the train from taking off again after a time-out without the doors having been opened? Otherwise it might just have kept on going. Seems like a good subject for the Kingston Trio.

Headless horseman? Horseless headman? Watch the driver putter? PGN]

---

### **✂ Shuttle roll incident on January '90 mission**

*<henry@zoo.toronto.edu>  
Fri, 13 Apr 90 22:16:19 EDT*

As many people know, during the LDEF retrieval mission in January 1990, at one point when the crew were asleep, a garbled "state vector" uploaded to Columbia caused the orbiter to start rotating. The extent of this has been somewhat exaggerated -- maximum speed was half an RPM, and the crew didn't notice until Mission Control woke them up -- but it was a bit startling that such a thing could happen. It could have been serious if it had happened at a worse time.

Most software people, on hearing about, react with "haven't those clods ever heard of checksums?". Well, it turns out they have. In the latest issue of World Spaceflight News (an excellent source for serious technical detail on shuttle flights), the full story is given. The telemetry channels were noisy at the time, the state vector was garbled by several noise "hits", and Mission Control's computers correctly announced that the copy sent back by the orbiter for confirmation didn't match the original and the state vector should be discarded. The ground controller responsible for the matter examined the detailed report, incorrectly decided that nothing important had been damaged -- and ordered the orbiter's computers to begin using the defective state vector! The orbiter, naturally, obeyed. In other words, this was ultimately operator error. The controller's action was "clearly outside the expected" procedures. (The question of whether this sort of thing is routine practice was not addressed, but I for one would suspect that the controller wouldn't have done that if he hadn't had to use manual overrides before.)

Procedures have been changed as a stopgap, and various long-term fixes are being considered, including the possibility of "inhibiting" the manual override in such cases. (It is not clear whether this means making it impossible, or just requiring some degree of confirmation or authorization.)

Henry Spencer at U of Toronto Zoology      uunet!attcan!utzoo!henry

---

### **✂ Software failures on Boeing 747-400?**

*"Trevor Warwick dtn: 830-4432 16-Apr-1990 1730" <warwick@marvin.enet.dec.com>  
Mon, 16 Apr 90 09:53:30 PDT*

Last week, I caught the end of an item on the BBC TV news where they were talking about a software fault that had been found on British Airways' new Boeing 747-400s.

Apparently, on more than one occasion, the flight control system had throttled all four engines back to idling speed while the aircraft was climbing. On each occasion, the pilot immediately intervened, and successfully rectified the situation.

It was then stated that after investigation by BA and Boeing engineers, a fault was corrected in the control software. Boeing was quoted as stating that they could not absolutely guarantee that faults like this would not occur again.

Can anybody supply any further details ?

For the record, I'm not overly worried about the increasing computerisation of aircraft systems. With today's software technology, I don't see how you can avoid incidents like the one mentioned above, and I wouldn't be stupid enough to claim that you could build a completely reliable system.

However, on balance, I think that the automated systems are an improvement, since they go some way towards eliminating the main cause of accidents, which is human error on behalf of the pilot. It may be that human error on behalf of the software engineer causes a different class of fault than you expect a pilot to make, but just because a fault is bizarre doesn't necessarily make it more dangerous.

The only reason I wouldn't fly across the Atlantic in an A320 is because it doesn't have enough engines !

Trevor Warwick

Telecommunications and Networks Engineering, Digital Equipment Corporation,  
Reading, England. warwick%marvin.enet@decwrl.dec.com

["the opinions expressed herein do not necessarily reflect the views  
or opinions of Digital Equipment Corporation"]

---

## **✂ False 1099 forms**

*Phil R. Karn <karn@thumper.bellcore.com>*

*Tue, 17 Apr 90 21:45:17 EDT*

Monday's Wall Street Journal carried a front page article about a new tactic being used by some hard-core tax protesters against the IRS: the filing of false 1099 forms. (IRS form 1099 is used to report miscellaneous payments to individuals; anyone who has done independent consulting should be familiar with them.) The targets of the false 1099s were generally enemies of the tax protesters: employees of the IRS, Federal judges, etc. The intent was apparently to cause grief for the victim when the IRS inquires why he or she didn't report the "income" on his or her tax return. The reported "amounts" ranged from thousands to tens of millions of dollars.

Although in principle this type of attack does not require the involvement of a computer, apparently the IRS has in recent years begun to conduct large scale computerized cross-checks between 1099 reports and the tax returns of the payees to see if miscellaneous income was properly reported. A sufficient number of false 1099 forms might seriously diminish the cost-effectiveness of this technique because of the need for manual verification of the forms. (The article quoted a former IRS commissioner as saying that this type of attack had the potential of becoming a "stick of dynamite" in the tax system.)

One wonders if there may be a fundamental limit on the degree to which institutions that must be open to many sources of public input can rely on a high degree of computerization to achieve cost-effectiveness, especially when the institution or its policies are unpopular. Local police and fire departments have long faced the problem of false alarms and malicious reports. They seem to deal with the problem by screening calls with human operators and by resigning themselves to wasting a certain percentage of their resources responding to crank calls. Credit reporting systems must also be open to many sources of input, and they too are often deliberately fed garbage.

Closer to home, computer networks such as Internet, phone BBSes and even "Sneakernet" represent social institutions through which people can contribute software, data and so forth, with the goal of increasing the cost-effectiveness of computer systems in general. But the Internet worm and especially the PC virus problem may mean that there is a fundamental limit on the degree of sharing, because of the effort that each individual must spend to ensure that he doesn't pick up an infected program or leave his computer open to network attack.

Although privacy and authentication mechanisms do exist, so far they seem to be workable only when the "community" within which the mechanisms are used to grant trust is relatively small, and threat of sanctions are effective in deterring abuses of that trust.

In the case of 1099 forms, anyone buying the services of an individual US resident is apparently required to file them, and that takes in an awful lot of corporations, small businesses and even individuals. Some may be in other countries. Even if each filer of 1099 forms were given an authenticator of some kind by the IRS, there would be little to keep someone from applying for such an authenticator under a false name. (In the cases cited in the WSJ article, a number of criminal prosecutions are underway, apparently because many of the perpetrators used their own real names as the payers!)

In the computer field, I'll leave it to your imagination as to how easy it is to find the author of a PC virus. Those few suspects that have been caught seem to have been extraordinarily careless in leaving evidence and witnesses around. I venture to guess that had Robert Morris developed his worm on his own computer in complete secrecy, we'd still be wondering who did it.

Phil

---

**🔥 Re: Risks [9.080] of Daylight Savings Time**

"zmudzinski, thomas" <zmudzinskit@IMO-UVAX.DCA.MIL>

16 Apr 90 14:53:00 EDT

One counter question, when did the railroads stop running on Standard Time?

(The transcontinental railways were the main reason we went to Standard in the first place. The last time I rode a train (not recent I'll admit), they still ignored local vagaries like Daylight Saving, War, Victory, etc. Time.)

/z/

---

### **✂ Re: Risks [9.080] of Daylight Savings Time**

Chuck Weinstock <weinstoc@SEI.CMU.EDU>

Wed, 18 Apr 90 09:31:13 EDT

The railroads went (mostly) to daylight time in the 1960's as best I can tell. I have some employee timetables that indicate that they go into effect at 12:01am (or 2:01am) Pacific Standard Time, on the Sunday of the time change, yet seem to have times in them on daylight savings time. I also looked at an old Official Guide from the 60's and it had some railroads showing their schedules in DST and others in ST. Amtrak, at least, publishes its schedules according to local time (when the computer doesn't goof!)

Side note: most railroads today don't publish times in their employee timetables (and they don't have public timetables since Amtrak). The reason for this is that with the increasing use of radios, it is typically more efficient to run all trains as "extras" and let the dispatcher sort out which train meets which train and where. The capacity of the railroad is increased. The exception is an Amtrak train, which always runs to a schedule.

Chuck

---

### **✂ Comment on UK Software Standards [[RISKS-9.1](#) and 2]**

<Richard Morton via PGN>

[lost, but old]

I have been following the discussion on the RISKS Forum regarding the new UK defense software standards, and it seems to me that the arguments about what technology should be in the standards are irrelevant. The standards as described by Sean Matthews ([RISKS-9.1](#)) appear to address only technical concerns (what programmers should do), and as such will never lead to higher quality systems regardless of which technology they espouse. Quality is first and foremost a management problem, not a technical problem. Long before we worry about the technology, we need to learn some basic management principles and apply them. David Parnas recognizes this when he writes:

I believe that organisations such as MoD would be better advised to introduce regulations requiring the use of certain good programming

techniques, requiring the use of highly qualified people, requiring systematic, formal, and detailed documentation, requiring thorough inspection, requiring thorough testing, etc. than to introduce regulations forbidding out the use of perfectly reasonable techniques.

Fred Brooks tried to make the importance of management clear in *The Mythical Man-Month*. For example, he noted "More software projects have gone awry for lack of calendar time than for all other causes combined." There is not even a hint of a technical problem there. He explains:

I believe that large programming projects suffer management problems different in kind from small ones, due to division of labor. I believe the critical need to be the preservation of the conceptual integrity of the product itself.

That book is almost 15 years old, and very few people seem to have taken it to heart. Marketing concerns still dominate schedule estimates on competitive contracts. Project managers still add more people to late projects. It seems like no one is listening. Apparently, we still haven't gotten the attention of top management. Why not try something different, something so simple any CEO can understand?

Henry Ford once recommended to Congress that all that was needed to solve the water pollution problem was to require people who take water out of a river to return it upstream from where they take it out. I believe that a similar simple but elegant solution to the "software problem" exists. Only one quality standard is required: Any company bidding on a high risk project (or better still, any project) must be able to demonstrate (and continue to demonstrate during the life of the contract) that the quality of their software development process is better this year than it was last year.

It does not do any good to try to tell people how to solve the problem, until it is their problem. Some people call this the 2-by-4 theory of how to get someone's attention. After they have been hit right between the eyes, they will ask us for the technology we have been trying to give them for the last 20 years.

Richard Morton, Institute for Defense Analyses  
(Opinions expressed are strictly my own.)

---

## **✂ Automates Fast Food**

*David Bank <unkydave@shumv1.ncsu.edu>  
Sun, 15 Apr 90 01:49:19 EDT*

Recent articles by [davy@instd.sri.com](mailto:davy@instd.sri.com) and [webber@psych.toronto.edu](mailto:webber@psych.toronto.edu) reminded me of a story related to my by my girlfriend.

For a time, she worked at a Hardees restaurant in North Carolina. It is my understanding that this was one of their "flagship" operations as it was geographically close to the center of the Hardee's "empire" in Rocky Mount, NC.

The events here took place a number of years ago. This food store had registers installed that recorded all of the purchases, so that at the end of the day the manager could get printouts of all the data and make sure the till matched the sales reported and help keep inventory updated.

These registers were "linked" and could "talk" to each other. At the end of business each day, the manager would go to a register (it did not matter which one), punch in a numeric code, and ALL of the registers would start printing out ALL of the purchases they recorded that day.

Once this process was triggered, from ANY register, there was NO way to abort or stop it. The registers printed until they were finished, short of pulling the plug on the whole system (which would cause data loss, obviously).

One day, a recently discharged assistant manager went thru the drive thru at the beginning of lunch "rush hour." When he got to the window, he made a request of the person at the window which he knew would require them to leave their station. While they were gone, he leaned in the window, typed in the aforementioned code on the register, and drove off...leaving the registers at the store paralyzed as they printed out the morning's sales at the height of the lunch rush. The front line staff was reduced to taking orders on pads and hand-calculating the cost and applicable tax, having to constantly refer to the menus behind them.

Unky Dave



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 9: Issue 1

Thursday 6 July 1989

## Contents

- [Elevator inquest update](#)  
[Walter Roberson](#)
- [UK Defense software standard](#)  
[Sean Matthews](#)
- [Exxon loses Valdez data](#)  
[Steve Smaha -- and Hugh Miller](#)
- ["Managing risk in large complex systems"](#)  
[Bob Allison](#)
- [A "model" software engineering methodology?](#)  
[Rich D'Ippolito](#)
- [CERT Offline](#)  
[Edward DeHart](#)
- [Re: Audi 5000 acceleration](#)  
[Dave Platt](#)  
[Mark Seecof](#)  
[Michael McClary](#)
- [Info on RISKS \(comp.risks\)](#)

---

### Elevator inquest update

<Walter\_Roberson@CARLETON.CA>

Fri, 30 Jun 89 11:07:29 EST

Another two days of the testimony into the April 1st elevator fatality in Ottawa has revealed some interesting/ scary facts.

It seems that the elevator type in question had a known problem with potentially being able to move when only one of the two doors was closed. A repair which involved moving only \*one\* wire was known, and had been recommended by the manufacturer in 1978. The repair was not made until 4 days \*after\* the accident, 11 years later.

In the meantime, the ownership of the building changed hands (in 1980), and the maintenance company changed (in 1988). The government inspectors never noticed that the change hadn't been made (there are only 2 inspectors for the Ottawa area, which has 3000+ elevators), and the

new repair company didn't notice it either. The owner of the company that checked the elevator just 1 hour before the death \*was\* aware of the change notice, but, as he put it:

"Are you telling me 10 years after a letter comes out... I should remember that?" [...]

"I would assume in 1980 [when the building was sold -- WDR] all those changes would be made, let alone 1988 [when he took over maintenance]. I don't know of any way any elevator company could know about it all."

The scary part came at the end of yesterday's article:

"The inquest was told no maintenance records were available for the elevators, installed with building construction in 1973. Records are not required by the ministry and are often removed by maintenance companies if the contract expires in order to hinder the new contractors, Allan Maheral said."

[The Ottawa Citizen, 28 June 1989, p. B1, and 29 June 1989, pp. A1-A2]

Walter Roberson <Walter\_Roberson@Carleton.CA>

---

## **UK Defense software standard**

*Sean Matthews <sean@aipna.edinburgh.ac.uk>*

*Fri, 30 Jun 89 13:49:12 BST*

I have just seen a copy of the UK department of defence draft standard for safety critical software (00-55).

Here are a few high (and low) points.

1. There should be no dynamic memory allocation (This rules out explicit recursion - though a bounded stack is allowed).
2. There should be no interrupts except for a regular clock interrupt.
3. There should not be any distributed processing (i.e. only a single processor).
4. There should not be any multiprocessing.
5. NO ASSEMBLER.
6. All code should be at least rigourously checked using mathematical methods.
7. Any formally verified code should have the proof submitted as well, in machine readable form, so that an independent check can be performed.
8. All code will be formally specified.
9. There are very strict requirements for static analysis (no unreachable

code, no unused variables, no uninitialised variables etc.).

10. No optimising compilers will be used.

11. A language with a formally defined syntax and a well defined semantics, or a suitable subset thereof will be used.

Comments.

1. means that all storage can be statically allocated. In fact somewhere it says that this should be the case.

2-4 seem to leave no option but polling. This is impractical, especially in embedded systems. No one is going to build a fly by wire system with those sorts of restrictions. (maybe people should therefore not build fly by wire systems, but that is another matter that has been discussed at length here already). it also ignores the fact that there are proof methods for dealing with distributed systems.

5. This is interesting, I seem to remember reading somewhere that Nasa used to have the opposite rule: no high level languages, since they actually read the delivered binary to check that the software did what it was supposed to do.

6-7. All through the draft the phrase 'mathematical methods' or 'formal methods' is \*invoked\* in a general way without going into very much detail about what is involved. I am not sure that the people who wrote the report were sure (Could someone from Praxis - which I believe consulted on drawing it up - enlarge on this?).

8. this is an excellent thing, though it does not say what sort of language should be used. Is a description in terms of a Turing machine suitable? After all that is a well understood formal system.

10. Interestingly, there is no requirement that the compiler be formally verified, just that it should conform to international standards (though strictly), and not have any gross hacks (i.e. optimisation) installed. There is also no demand that the target processor hardware be verified (though such a device exists here already: the Royal Signals Research Establishment's Viper processor).

11. seems to be a dig at Ada and the no subsets rule. It also rules out C.

Conclusions.

I find the idea of the wholesale mayhem and killing merchants being forced to try so much harder to ensure that their products maim and kill only the people they are supposed to maim and kill, rather amusing.

The standard seems to be naive in its expectations of what can be achieved at the moment with formal methods (That is apparently the general opinion around here, and there is a \*lot\* of active research in program verification in Edinburgh), and impossibly restrictive.

An interesting move in the right direction but too fast and too soon. And they might blow the idea of Formal verification by trying to force it too soon. And I would very much like to see these ideas trickle down into the civil sector.

I might follow this up with a larger (and more coherent) description if there is interest (this was typed from memory after seeing it yesterday) there is quite a bit more in it.

Sean Matthews

Dept. of Artificial Intelligence JANET: sean@uk.ac.ed.aipna

University of Edinburgh ARPA: sean%uk.ac.ed.aipna@nsfnet-relay.ac.uk

80 South Bridge UUCP: ...!mcvax!ukc!aipna!sean

Edinburgh, EH1 1HN, Scotland

---

### **Exxon loses Valdez data**

*Steve Smaha <Smaha@DOCKMASTER.NCSC.MIL>*

*Wed, 5 Jul 89 11:58 EDT*

This appeared in the 2 Jul 89 Austin (TX) "American-Statesman".

"Exxon accidentally destroys data files on Alaska oil spill,"

by Roberto Suro, New York Times Service

HOUSTON - A computer operator at Exxon headquarters in Houston says he inadvertently destroyed computer copies of thousands of documents with potentially important information on the Alaskan oil spill.

A federal court had ordered Exxon to preserve the computer records along with all other material concerning the grounding of the Exxon Valdez in Prince William Sound on March 24 and the subsequent cleanup effort.

Les Rogers, a spokesman for the Exxon Company USA, confirmed the destruction of the computer records but said the oil company's lawyers believed other copies exist.

"Very early in the spill, even before the court order, Exxon took the initiative to instruct all its employees to save all documents relating to the event because of the anticipated litigation," Rogers said. "We assume these instructions have been followed."

The computer technician, Kenneth Davis, said that it would be difficult and perhaps impossible to determine what documents were on destroyed computer files.

Exxon faces about 150 lawsuits as a result of the spill, which dumped 11 million gallons of crude oil into Prince William Sound, and it appears certain that the loss of these documents will be the subject of court arguments.

Stephen Sussman, a Houston lawyer involved in a suit against Exxon on behalf of Alaska fishermen, Native Americans, and others, said, "The destruction of these records is potentially significant to our case in that we will be arguing that Exxon has been negligent throughout this disaster and now perhaps it was negligent even in the handling of its own documents."

Davis, 33, was dismissed June 8, the day after the destruction of the

records was discovered.

In several interviews, and in written statements to the Texas Employment Commission, Davis alleged that his superiors had been negligent in safeguarding the computer records and that his actions resulted from their failures.

The destroyed material included all internal communications and word-processing documents from both the Exxon Shipping Co., which owned the tanker, and the executive offices of Exxon USA.

Davis said that since the tapes were the only complete copy of what passed through those computer systems, it might be impossible to determine what was lost.

[The full NYT text was sent in by Hugh Miller <MILLER@vm.epas.utoronto.ca>, who prefaced the text with this reference to '1984' by George Orwell:

``I was thinking just this morning about how Winston Smith's job in historical engineering would have been a lot easier if everything had been kept on magnetic media, when this item appeared in today's NYT."`

To conclude, he made some comments about the difficulties of prosecuting after the documents have been destroyed (with reference to Ollie and Fawn).

``Want to bet Exxon doesn't use a PROFS system?''

---

### ✂ IEEE Spectrum June issue: "Managing risk in large complex systems"

<bobal@microsoft.UUCP>

Wed Jul 5 16:40:22 1989

The June 1989 issue of IEEE Spectrum contains a series of articles discussing risk management techniques and failures, paying particular attention to the areas of aging aircraft ala the Aloha Airlines 737 incident, the Hinsdale fire which shut down phone service near Chicago, the Savannah river nuclear reactors, the space shuttle, and the release of lethal chemicals in Bhopal.

Perhaps because of my own particular biases, the space shuttle article was particularly interesting where it describes the risk of a shuttle accident also dooming the space station (due to the destruction of single copies of critical space station components).

Bob Allison

---

### ✂ A "model" software engineering methodology? ([RISKS-8.86](#))

<rsd@SEI.CMU.EDU>

Mon, 03 Jul 89 14:46:23 EDT

In [RISKS 8.86](#), Jon Jacky quotes Stan Shebs:

We supposedly had a "model" software engineering methodology; what I remember most clearly is that half the work was done on one flavor of IBM OS, and the other half done on a different flavor, and file transfer

between the two was tricky and time-consuming.

The coupled clauses are unrelated, a compositional practice Mr. Shebs is apparently quite fond of. Let's concentrate on Mr. Sheb's text to see what his understanding of software development is:

The day-to-day work was [...] writing the "Program Design" for an already-written program (is that stupid or what), figuring out how to compute the intersection of two polygons in space.

Without context, this is not evidence that the SE method was good or bad. Of course the program design should have been documented beforehand, but recognizing that it is necessary to have for testing and maintenance purposes is not stupid. I have seen many systems where the software is very old (or inherited) and must be re-documented to current standards. What was the case here?

I suppose the greatest risk of failure derives from things that weren't anticipated during testing, such as a Siberian snowdrift changing the topography on a navigation map...

[How does the snow get on the map?!] One does not wait until testing to anticipate such contingencies. Does Mr. Shebs think so?

(Regarding) statistics on software quality, the closest thing we had was maybe a count of problem reports (hundreds, but each report ranged from one-liners to one-monthers in terms of effort required).

Sigh. There is no mention here whether this applies to delivered product or corrected production errors. Is this his view of what constitutes quality?

Nothing classified, we had the odd situation that the *\*data\** was [sic] classified, but the *\*program\** wasn't even rated "confidential"!

Odd situation? Apparently, Mr. Shebs had a single experience in the MCCR community.

This article was posted to illuminate "the accuracy/quality of strategic weapons guidance systems", presumably by offering a coherent and reasoned exposition. Instead, it presents jokes, innuendo, and unsubstantiated charges and conclusions in indefinite (and sloppy, such as the 1/2 inch diameter missile) language such as:

The difficulty of all this apparently didn't occur to anybody until after the missile was working...

...error accumulation over 2000 km is immense,...

...cute little cassette tapes...

The precision and formality of the software was very low, but it was exhaustively tested over and over and over again.

Really, if Mr. Shebs's rambling demonstrates anything, it shows that the greatest risk is hiring inarticulate and confused programmers like himself who don't have the faintest idea what software engineering is.

Mr. Shebs appears to come clean in only one statement:

The fragility of something like the cruise missile and its software is something I've spent a lot of time wondering about, and don't really have any idea.

Indeed.

Rich D'Ippolito

---

### **🚨 CERT Offline [Computer Emergency Response Team]**

*<Edward DeHart <ecd@cert.sei.cmu.edu> [forwarded via many different paths]>  
Wed, 5 Jul 89 14:19:09 EDT*

The supply of cold water to our air-conditioners has been turned off due to a major break in the pipes. The problem may not be corrected until the weekend.

The lack of cold water is bad news for the computer room. All of the systems are going to be turned off.

For the next day or so, CERT will not be able to send or receive EMAIL via the Internet.

We will be in the building if you need to contact us. Our telephone number is 412-268-7090.

Please forward this information to others in your group.

Thanks, Ed DeHart

[whhada yuh know; CERT needs a CERT! The police dept's computers are down ... Willis Ware]

[I suppose the famous detective, Air-Cool Pour-out, will investigate. PGN]

---

### **🚨 Re: Audi 5000 acceleration [[RISKS-8.87](#)]**

*Dave Platt <dplatt@coherent.com>  
Fri, 30 Jun 89 10:40:37 PDT*

- > The study, "An Examination of Sudden Acceleration," explored ...
- >
- > However, there was evidence of minor surges of about three-tenths of the
- > Earth's gravity for 2 seconds caused by electronic faults in the idle
- > stabilizer systems of the Audi 5000 ... the surge could startle a driver
- > enough to accidentally push the accelerator instead of the brake, ...

Minor?? .3G works out to roughly 10 feet/sec<sup>2</sup>, or a zero-to-sixty acceleration time of about 9 seconds. This may not be considered "full power" or "major" acceleration for a sports-car, but my old Volvo has difficulty reaching highway speed (55) in 9 seconds even if I floor the accelerator.

A .3G surge for 2 seconds would accelerate a car from a standstill to somewhere in the neighborhood of 20 feet/second, and would carry the car about 10 feet forwards. Startling? I should say so... especially to drivers who might have only recently switched to the Audi from an older, lower-powered car.

Even if this fault in the idle stabilizer cannot invoke "full" acceleration by itself, it sounds substantially dangerous in and of itself. Coupled with poor pedal/linkage layout and design, it apparently adds up to a real hazard.

Dave Platt FIDONET: Dave Platt on 1:204/444 VOICE: (415) 493-8805  
USMAIL: Coherent Thought Inc. 3350 West Bayshore #205 Palo Alto CA 94303

---

### ***#* misleading Audi surge report**

<icc.marks@SEAS.UCLA.EDU>

*Fri, 30 Jun 89 11:39:11 PDT*

Three-tenths of the Earth's gravity is not "minor." That's about three meters per second squared. At the end of two seconds the car would have travelled about six meters or twenty feet. 3m/sec<sup>2</sup> on a 1500 Kg automobile for just a moment will set it moving fast enough to squish or bash-in any likely obstacle (inertia, you know).

I'll bet drivers are startled! They aren't likely to accelerate that fast when parking... Sixty miles per hour is about a hundred kilometers per hour. That's about twenty-eight meters per second. At 3m/sec<sup>2</sup> it takes only nine or ten seconds to reach 28m/sec; the owners of Audi 5000's are probably pleased with the "zero to sixty in six seconds" performance of their cars; that's less than 5m/sec<sup>2</sup>. (Many cars can't do 0-60 in less than 9 seconds flat out.) This means the "surges... caused by electronic faults" are equivalent to accelerating away from a stop light in traffic--and only a third less than flooring the gas pedal to get onto the Pasadena Freeway in Highland Park. Imagine if you were easing your car into your garage at an idle and it suddenly accelerated like you were taking off from a stop sign.

(Before you all write to criticize the math, I'm aware that I've neglected air resistance and gear shifting, but I don't think this invalidates the

discussion.)

If the report does minimize the fault in the Audi's electronic controls to lay the blame on the driver, then we must ask whether the authors wanted to shift concern away from Audi where it seems to belong. (No, I've never owned or even driven an Audi.)

Mark Seecof, Locus Computing Corp., Los Angeles (213-337-5218)  
My opinions only, of course...

---

✉ **Audi surges (Re: [RISKS DIGEST 8.87](#))**

Michael McClary <michael@xanadu.COM>  
6 Jul 89 18:06:27 GMT

>However, there was evidence of minor surges of about three-tenths of the  
>Earth's gravity for 2 seconds caused by electronic faults in the idle  
>stabilizer systems of the Audi 5000

Is this a missprint? I find the characterization of a two-second, 3/10 g surge as "minor" to be ludicrous.

This is especially true if it is the result of a malfunction in an idle speed control system, implying that it would occur when the vehicle was stopped. At a busy intersection, for instance, with pedestrian cross-traffic or another stopped car just a foot or two ahead.

After one second, a 3/10g surge would have moved the vehicle almost five feet forward, and have it traveling over 6 1/2 MPH. By the end of the two second surge, if nothing is done, the car would be doing 13 MPH and have gone nearly twenty feet.

No hypothetical "pedal misapplication" is necessary to make such a vehicle hazardous, and while zero-to-sixty in under ten seconds may not be full throttle for an Audi, it's close enough for me.



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

**Volume 9: Issue 82**

**Friday 20 April 1990**

## Contents

- [A320 news](#)  
[Henry Spencer](#)
- [The Danger of Airbags](#)  
[Jeff Deifik](#)
- [Re: Risks of computerized publishing](#)  
[Paolo Mattiangeli](#)
- [Postal Employees and cross-matching](#)  
[Brinton Cooper](#)
- ["It's a Computer Error"](#)  
[Lindsay F. Marshall](#)
- [Re: London Tube Train](#)  
[Clive Feather](#)
- [London Underground Low-Tech](#)  
[anonymous](#)
- [Virus outbreak in China!](#)  
[R.Gowans via MCGDRKG in Virus-L](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ***✉* A320 news**

<[henry@zoo.toronto.edu](mailto:henry@zoo.toronto.edu)>

Thu, 19 Apr 90 00:23:29 EDT

The latest A320, um, news, from Flight International 14 March...

As most readers know, the official conclusion of the inquiry into the first A320 crash (the airshow at Habsheim in 1988) was pilot error: they were flying too low and too slowly with engines at very low power, and increased power too late to avert the crash. This was corroborated, in detail, by the flight data recorder and cockpit voice recorder.

The pilots have recently been charging that the FDR and CVR recordings were tampered with by the investigators. The last straw, apparently, came when the pilots' lawyer asked India's prime minister to keep the French investigators

away from data on the Bangalore crash on grounds that they might tamper with it too...

The French Minister of Transport, his Director of Civil Aviation, and the head of the accident-investigation office are suing the pilots for libel.

Henry Spencer at U of Toronto Zoology    uunet!attcan!utzool!henry

---

### **✉ The Danger of Airbags**

*Jeff Deifik <JDEIFIK@ISI.EDU>*

*Wed 18 Apr 90 10:24:43-PST*

Recently, I saw an airbag malfunction. I was with the Porsche Owners Club at Willow Springs International Raceway. A 1989 Porsche 944 turbo was braking, going downhill, when a grey cloud of smoke came out of the passenger compartment. The airbags had gone off, but fortunately the driver didn't lose control. The front windshield was broken from the passenger side airbag, and the driver's arm was bruised. The driver had the traditional safety equipment including, including 6 point harness, helmet, and fire-resistant gloves, suit, and shoes. I suggested that the sensors be tested or replaced, or that the system be disabled. The car had sticky, but street-legal tires. The estimated cost to repair was \$1000. The car was out of warranty, but the driver said he hoped Porsche would pay for it. The RISKS are obvious.

Jeff Deifik jdeifik@isi.edu

---

### **✉ Re: Risks of computerized publishing (Spencer, [RISKS-9.80](#))**

*Paolo Mattiangeli <MERCEDES@IRMUNISA.BITNET>*

*Wed, 18 Apr 90 18:42:25 ITA*

I wonder if I'm in mistake when I think that such things aren't essential faults of computerization. This kind of mistakes depend, in my opinion, on people using computers in a silly way, giving the machine inappropriate responsibilities. If a publisher sets a book for publishing in a traditional way, he double-checks the films before sending them to the printer; it seems that computerized publisher do not. I think this is misunderstanding what a computer can do.

---

### **✉ Postal Employees and cross-matching**

*Brinton Cooper <abc@BRL.MIL>*

*Thu, 19 Apr 90 9:41:28 EDT*

>From the "Weekly Federal Employees' News Digest":

The US Postal Service this month will begin checking its payroll records to identify employees who are delinquent on government payments for various

reasons. The computer matching will continue for 18 months.

USPS is combining its data banks for individuals who are late paying on Housing and Urban Development Department loans (including housing assistance), certain veterans benefits, student loans, Small Business Administration programs, loans from the Agriculture Department and the Department of Health and Human Services and for exceeding salary limitations under the dual compensation law.

USPS published details of these and other USPS computer matching efforts in the March 20 Federal Register. USPS listed Betty Sheriff as a contact at: (202)268-5158."

---

### **✉ "It's a Computer Error"**

*"Lindsay F. Marshall" <Lindsay.Marshall@newcastle.ac.uk>  
Thu, 19 Apr 90 15:13:41 BST*

I have noticed a recent upsurge in UK news reports of "Computer Errors". Not of the major catastrophe kind, but of the "bill for \$0.00" sort. This seems to be intimately related to the introduction of the Poll tax. I wonder if any other RISKS subscribers have noticed this phenomenon (not the poll tax, the computer errors) ?

Lindsay

Lindsay.Marshall, Computing Laboratory, The University, Newcastle upon Tyne, UK  
NE1 7RU +44-91-222-8267

---

### **✉ Re: London Tube Train ([RISKS-9.81](#))**

*Clive Feather <clive@ixi.UUCP>  
Thu, 19 Apr 90 07:42:20 bst*

> But he was certainly optimistic to think that he could CATCH UP with his  
> train, since the automatic controls clearly are designed to prevent that.

The following train would have been allowed to proceed up to about 100m behind his train, which would be sitting at the next station (Pimlico). He could then have walked along the track and boarded it (there is a door in the front of the driver's cab). I hope the driver of the second train would have turned off the automatics when he did this :-)

> Actually, the train is not COMPLETELY automatic; the opening and closing of  
> doors is controlled manually. But perhaps there is an interlock that keeps  
> the train from taking off again after a time-out without the doors having  
> been opened? Otherwise it might just have kept on going.

Once the train has received an "at station" signal from the track, the automatic system is turned off. To turn it back on again, the following must hold simultaneously:

- the cab windows are proved to be shut (microswitches, I presume)
- the track is sending code 4200 (start train, accelerate to 80 km/h)
- the driver is pressing both START buttons

It would appear from the above incident that "train doors shut" is tested further down the logic, so there is a RISK here.

Clive D.W. Feather, IXI Limited, 62-74 Burleigh Street, Cambridge U.K.

---

## ✂ London Underground Low-Tech

<anonymous>

Thu, 19 Apr 90

Recently there was a question in this forum regarding how much control the operator of a train in the Underground has over the system. This was in regards to the near head-on collision that was avoided when the operator on one train saw approaching headlights and "shut down" the train power locally.

This is actually accomplished through a wonderfully low-tech system. If you have ever ridden the Underground, you may have noticed a pair of bare wires mounted on the wall of the tunnel that is always zipping by. That pair of low-voltage wires fulfills two functions. First, it provides an emergency communications path. An operator can simply reach out of his window and clip a lineman's test set phone (or similar device) onto each lead and be in communications with a central point.

Secondly, if the wires are SHORTED together (there is enough slack in the mounting to make it possible to do this easily with your hand through the operator window), power is automatically cut to the section of track in the area where the short was applied (the power is restored through manual operations later). Simple, and it WORKS!

The Underground is loaded with all sorts of nifty low-tech operational control and safety systems that have been in use for many, many decades (remember that the Underground was the first real subway system in the world) including some wonderful old lifts. When in London, be sure to check out the London Transport Museum as well!

---

## ✂ Virus outbreak in China! (PC)

<MCGDRKG@CMS.MANCHESTER-COMPUTING-CENTRE.AC.UK>

Wed, 18 Apr 90 20:43:00 -0000

[FROM VIRUS-L Digest Friday, 20 Apr 1990 Volume 3 : Issue 78]

I thought I would forward this to the group as a matter of interest. It was taken from JBH Online (Wed. 18th April 1990)

----- Start of forwarded note -----

China: Computer viruses reported

BBC

The China Daily newspaper reports that a large scale infection of the country's computers began last Friday, 13 April, when several computer viruses, including the Jerusalem virus, are believed to have been time activated. At least six separate computer viruses have been identified in Beijing alone. The BBC is introducing its report of the China Daily story by referring to the large scale infection as "sabotage."

R.Gowans, Dept Civil Eng, U.M.I.S.T, Sackville Street, Manchester M60 1QD 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 9: Issue 83

Wednesday 25 April 1990

## Contents

- [You think YOU have problems with your telephone company?](#)  
[PGN](#)
- [Traffic light outages](#)  
[King Ables](#)
- [Sabbath Goes High-Tech](#)  
[David Dabney](#)
- [Computers and Hyphenated names](#)  
[Allan Meers](#)
- [London tube train and the Boeing 747 ...](#)  
[Clive Walmsley](#)
- [Risky McDonald's comrade...](#)  
[David Gursky](#)
- [Risks of engine computers and EMP](#)  
[Lynn R Grant](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **✉ You think YOU have problems with your telephone company?**

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

Tue, 24 Apr 1990 15:45:46 PDT

A woman in Kissimmee, Florida, sent me a dossier that she has compiled over the past few months, carefully documenting an alarming sequence of problems. It is one of the most bizarre cases I have ever seen. The problems are still continuing, unresolved.

She runs a business out of her home, and has an 800 number that rings onto one of her two home phones -- although the problems began BEFORE the 800 line was connected. Her local phone company is United Telephone Company. The list of anomalous events is somewhat incredible, but is supported by many witnesses, including law enforcement people. It includes the following types of incidents.

Calls billed to her 800 number from parties that never called her (in one

case from a phone in Chicago that was not equipped for outgoing calls!).

Calls billed to one of the home phones when there was no phone activity, that is, for calls that were never made to people who never received them.

These troubles with the phone company have resulted in huge bills for calls that apparently were never made. Even more fascinating incidents were these:

Frequent incoming calls that were wrong numbers -- usually in large batches on the same day -- to similar 800 numbers, originally THREE numbers in particular, and then suddenly TWO new numbers after some problem was allegedly fixed.

With alarming frequency, apparently crossed lines resulting in two parties BOTH getting ringing tones, answering, and finding themselves talking to each other.

Crossed lines such that multiple conversations could be heard clearly at the same time.

Repeated calls to 911 attributed to her phone, even when no one was home.

The most interesting and best documented single incident was probably this:

On 27 Feb 90, a local Kissimmee police officer was in the house trying to make sense out of what was going on. ``He picked up the phone and dialed the police department, however he reached Yellow Cab. He put down the phone ... not understanding how he reached the Yellow Cab company when [about three minutes later] the telephone rang and [the officer] answered the phone only to be connected to a Howie, a dispatcher at the police department, only neither of them had called one another..."

It's only a software problem? With remotely reprogrammable call forwarding, speed dial, redial, automatic dialing units, etc., in central offices, almost anything seems possible these days, especially when you consider the possible interactions among these features. One could program up some of the above incidents as combinations thereof. However, she did not subscribe to any of these features -- although the mechanism to turn them on is itself programmable.

If these were the only problems, the logical choice would be a messed-up central office and monumental incompetence on the part of the telephone company in fixing the problems. Apparently the telephone company has been baffled, with even the trap-and-trace efforts seemingly not having been consistent with observed reality. Some observed calls were not trapped, and some trapped calls were never placed! But compounding the situation have been a variety of apparently genuine threatening and/or harassing phone calls. From that we consider the tentative conclusion that there are either at least TWO COMPLETELY INDEPENDENT PHENOMENA, telephone system problems plus malicious human agents, or ONE SET OF INTERRELATED PHENOMENA caused by a malicious person who has access to and knows the telephone hardware/software system, with any of a variety of motives. I have several (unpublished) reports about how easy it is for outsiders to hack telephone switches, but it is obviously even easier when an insider is involved.

The RISKS archives include quite a few cases of intentional hacking of telephone systems, as well as numerous cases of accidental misbilling and other screwups. But above all, RISKS readers know how easy it is for things like that to happen.

Is it possible that we might be able to provide some help for this person in Kissimmee, who seems to be a victim of many problems -- including the "computer is never wrong" syndrome on the part of the telephone company, whose employees have had difficulty believing that any of these things could actually happen?

My main question to you all is this:

Do you know of other cases of unintentional (or intentionally caused) rampant deviations from expected normal behavior that have been attributable to a telephone system and its operation, as a result of scrambled software, miswired switching gear, inept personnel, etc.? Has anything like this happened to you?

Please try to provide as much detail as possible. Also, avoid speculation on this particular case unless it is VERY WELL INFORMED. The dossier is very thoughtfully constructed, and the complexity of the case suggests that an adequate explanation may be nontrivial, although -- as we all know by now -- a small software flaw can go a long way. PGN

[P.S. I have omitted her name and phone numbers, because that might only tend to worsen the problem for her, and for you -- were you to call her.]

---

## **✂ Traffic light outages**

*King Ables <ables@mcc.com>*

*Sat, 21 Apr 1990 12:40:46 CDT*

Well, last month (Rich Neitzel, in [RISKS-9.73](#)) we read about Lakewood, Colorado, where the computer controlling the town's traffic light system lost a disk and all the traffic lights in town went to blink.

I said then I couldn't believe that not only did they not have a duplicate machine they could quickly pull in for use, but that when the traffic signals got confused, they didn't simply go to some "sane" cycle of green-yellow-red even if it wasn't timed the way it should be for various intersections.

I spoke too soon. On Good Friday (Friday the 13th, no less) we experienced the same thing here in Austin. Apparently some software was modified and the changes were loaded without the proper testing. The next day (Friday) at noon, the system sent out incorrect information to about 60% of the traffic signals in town (about 360 or so). Apparently, when a traffic signal here get confused (or receives bad information), it is supposed to go to a red/yellow blink (or red/red depending on the intersection). As long as only one signal gets bad information from time to time, this works okay. But when the bad information originates at the controlling system, all hell breaks loose! Of course, traffic ground to a halt and there were accidents all over town (I never heard a final count of accidents, but they were still counting the reports Saturday

afternoon).

I had the bad luck to have Friday off, so of course, I was out trying to run errands and such.

City crews had to drive around town and manually reset the lights at the site. It seems after a light gets bad information, it just listens for any other information and has to be manually reset! Does this seem like a really BAD idea to anybody else?

So I guess I should be more careful before I go pointing my finger and saying "they" deserved what they got in Colorado! Are all traffic signal systems designed this poorly? Maybe that's a good area to get into right now!

The official word was untested software. It still seems REAL suspicious to me that it happened almost exactly at noon on Friday the 13th. I can't help but wonder if there was a reason for that.

But my original point still stands. We rely on computers too much to simply "believe" that the answer they provide will always be right, because just like anything else, computers fail. The biggest danger we face is people believing in them TOO MUCH.

King Ables, Micro Electronics and Computer Technology Corp.  
3500 W. Balcones Center Drive, Austin, TX 78759 +1 512 338 3749

---

## ✂ Sabbath Goes High-Tech

David Dabney <ddabney@hal.unm.edu>  
Sat, 21 Apr 90 15:16:41 MDT

This is a summary of an AP story from Jerusalem, from the Albuquerque Journal ('about 3 weeks old', says David. Stark abstracting by PGN)

### ISRAELI RABBIS ADAPT STRICT SABBATH LAWS TO HIGH TECHNOLOGY

For modern convenience, there is now a "Sabbath timer" to control lights, hot plates, hot water heaters, and other devices that under strict laws should not be touched on the Sabbath.

``Though most people use simple, inexpensive timers like those commonly installed in video recorders, some Jerusalemites have now built elaborate, computer-controlled timing systems into their homes. In one luxury home built by an American immigrant, the computer switches the hot-water supply from electric-run boilers to solar heaters on Saturdays, thus avoiding trespassing of custom. Of course, there are those accused of abusing the system. "I know some guys who arrange for the TV to come on just in time for the ball game," said one American-born woman who restricts her timers to lights."

The article also included some discussion on koshering a microwave, and on interpreting old laws in terms of modern technology.

---

## ✂ Computers and Hyphenated names

Allan "I like broccoli" Meers <allans@EBay.Sun.COM>

Sun, 22 Apr 90 23:10:03 PDT

Since your Social Security number is quickly becoming our National Identification Number (IRS wants one for 2-year-olds and up), they might as well get used to hyphenated names, really long names, multiple name changes, and one-word names.

[... not to mention intermediate upper-case letters that change the parse, Swedish vowels, and perhaps eventually further nonalphabetic characters such as in some of the net addresses I have to put up with (":", "#", "^"), etc. PGN]

Dear Abby,

When my husband and I were married, I chose to retain my last name. When our son was born, we decided to give him a hyphenated last name, using both our names. Came time for our son to get a Social Security number, we learned that there was no hyphen in his last name. I called the Social Security office and was told, "Our computers cannot put hyphens in names".

This was very frustrating. If two names are seperated by a space instead of a hyphen, the name is alphabetized incorrectly; if two names are joined together, everyone mispronounces the resulting name. Wouldn't you think that in the day of technological mircales, someone could make it possible for hyphenated names to be recorded correctly on our official documents?

Barbara - Oakhurst, California

Dear Barbara: Someone has. The symbol for the hyphen was programmed into the Social Security computer in August 1988. Contact your local Social Security office and request your son's hyphen.

[Perhaps they thought she wanted a Haifan? Or `Und der Hyphisch?' PGN]

---

## ✂ London tube train and the Boeing 747 ...

"Clive" <walmsley@ccint1.rsre.mod.uk>

23 Apr 90 10:01:00 WET DST

I could not help smile at the two unrelated articles in [Risks 9.81](#). These are of course the London Tube train incident and the software failures on the Boeing 747-400.

One wonders how long it will be before we read of an incident where a passenger carrying aircraft takes off leaving the pilot on the ground !!!

Clive Walmsley

[I try not to edit contributions too much, but I could not help (but)

smile at the notion of a passenger carrying more than one aircraft and thought that the passenger might deserve a hyphen. But I resisted inserting it. Sorry. PGN]

---

### **✂ Risky McDonald's comrade...**

*David Gursky <dmg@lid.mitre.org>  
Tue, 17 Apr 90 07:54:47 EDT*

The ironic portion of the story of McDonald's new store in the Soviet Union is that the Russians are right. The most efficient way to process the large queue of people is with one queue and multiple servers, not the way McDonald's traditionally does it with multiple queues and multiple servers.

---

### **✂ Risks of engine computers and EMP**

*Lynn R Grant <Grant@DOCKMASTER.NCSC.MIL>  
Sun, 22 Apr 90 20:34 EDT*

I just got done pouring a bunch of money into my car because the engine computer died, and it got me thinking about the vulnerability of modern car engines.

In the event of a nuclear explosion, the resulting EMP (electromagnetic pulse) would not only wipe out a lot of semiconductor-based communications gear, it would also kill the engine computers in every late model car. And what about the Military? I used to work for a big-3 truck manufacturer, and the trucks we built for the Army looked pretty much like our regular trucks (except for the cammo paint jobs) and were build on the same assembly lines. I wonder if they used the same computer-based engines? If a tactical nuclear strike could wipe out all the vehicles in the area, that's a rather scary thought, eh?

This is all speculation on my part. If anyone out there knows how real this vulnerability is, I would be interested in hearing it.



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 9: Issue 84

Thursday 26 April 1990

## Contents

- [Re: You think YOU have problems with your telephone company?](#)

[Gary Chapman](#)

[David G. Novick](#)

[Vincent](#)

[Laura Halliday](#)

[Al Stangenberger](#)

[Pete McVay](#)

[John Higdon](#)

[Greeny](#)

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

---

### ✉ Re: You think YOU have problems with your telephone company?

Gary Chapman <[chapman@csl.stanford.edu](mailto:chapman@csl.stanford.edu)>

Wed, 25 Apr 90 11:37:36 PDT

The telephone system in Kissimmee sounds like the one in Moscow (the one in the Soviet Union, not in Idaho). Callers in Moscow are constantly getting wrong numbers, and those who have telephones are constantly interrupted by the telephone ringing, usually with someone who has reached the wrong number. I have heard people in Moscow say that the chance of getting the number that you dialed is 50-50, and this is something that everyone has learned to live with.

As I discovered in my hotel in Moscow, the people who do ring through to your telephone unintentionally are rarely surprised and never apologetic--in fact, they are frequently quite chatty. A strange form of social communication between strangers.

Here's a story from Moscow, which is apparently fairly representative:

A man lives in an apartment building with only one telephone serving about a hundred residents. One day there is a fire in the building. The man rushes to the telephone to call the fire department. He picks up the telephone and is inexplicably connected to his workplace, and his boss is on the line. The man

is momentarily flustered, the boss says, "How nice to hear from you." The man is a little stressed, trying to figure out how to get through to the fire department before the fire gets out of control.

Man: "I'm sorry. . . "

Boss: "You sound upset. What's wrong?"

Man: "We have a situation here."

Boss: "What do you want me to do?"

Man: "Nothing."

Boss: "Then why did you call me?"

I'm sure there are many more amusing (and not so amusing) effects of having a telephone system that is so unpredictable. The Soviet telephone system is non-digital, of course, and still uses old cross-bar switching. This is unlikely to be the problem in Kissimmee, but the problems sound similar.

Gary Chapman, Executive Director, CPSR

---

### **✂ Re: You think YOU have problems with your telephone company?**

*"David G. Novick" <novick@cse.ogi.edu>*

*Wed, 25 Apr 90 15:42:33 -0700*

I had first-hand experience with a single instance of a very similar problem. This occurred in the U S WEST Communications phone system for Eugene, Oregon, around 1988.

A friend of mine called me from his home. A little later I returned the call. Instead of any normal response, the phone system responded with the out-of-service message: three loud tones followed by "The number you have called has been disconnected or is out of service..." On a couple of subsequent tries (motivated by suspicion that I made an error, followed by disbelief), I always got the same message. Eventually I called an operator to complain.

It turns out that my friend's phone had been forwarded to another number, despite the facts that (1) the other number was not a working number and (2) my friend did not have call forwarding. It seems to have been an internally generated system error. A disturbing aspect of this is that my friend could always call out, so that his phone seemed to be working; it's just that no-one ever seemed to call them. It is unknown how long this state had existed. Indeed, if the number to which the calls were being forwarded was a working number that turned out to be either always busy or not answered, this situation might have continued indefinitely.

David Novick

Department of Computer Science and Engineering, Oregon Graduate Institute of Science and Technology, 19600 N.W. Von Neumann Drive, Beaverton, OR 97006-1999  
(503) 690-1156

---

**✉ Re: You think YOU have problems with your telephone company?**

<vincent@neat.cs.toronto.edu>

Wed, 25 Apr 1990 18:23:52 -0400

Several years ago (1984) I worked as a summer student in Bell Northern Research (which is the research arm of Northern Telecom and has nothing to do with Bell in the states). At the time they decided to field test one of their new SL100 switches (hope I have the right number) by making the people who made it live with it.

Anyway, for the first month or so after the introduction of the system we experienced problems very similar to the ones mentioned. I personally experienced the "match-making" phenomena of having the phone ring, hearing it ring on the other end and then having someone else answer. Very weird.

Phone calls would not only fail, but were misdirected and at times switched. Most of these glitches ended quite quickly but it took a month or two for everything to settle down. This was the first phone system that I had dealt with that had all those nice features which phone companies are starting to offer: call forwarding, call park, speed dial directories stored off the handset etc. I'm sure that interactions between these features contributed to the problems. Perhaps someone at BNR remembers this episode and actually knows something about why it happened. It may be worth trying to contact them, especially if it is one of their switches.

Vincent

P.S. This occurred in the first few months of 1984 and it did send a good Orwellian shiver up my spine.

---

**✉ Re: You think YOU have problems with your telephone company?**

Amos Shapir <amos@nsc.UUCP>

Wed, 25 Apr 90 14:29:28 -0700

In Israel the (government owned) company is notorious for such incidents. Where I live, connections to numbers in Tel Aviv starting with 4, especially 41 and 42, are sometimes close to impossible, with all the phenomena you mentioned, especially cross-talk between lines. The common explanation is that this is an old exchange which is overloaded. In any case, all this is caused by bad hardware, mainly due to rain damage (when it rains, they have to wait until the lines are dry before fixing anything; but then they don't know where the cracks are!).

There are new and computerized exchanges too, but the only difference seems to be that there such malfunctions are echoed into billing too, and of course, they blame the computer for \*everything\*.

Amos Shapir

National Semiconductor, 2900 semiconductor Dr., Santa Clara, CA 95052-8090  
Mailstop E-280 amos@nsc.nsc.com until May 1, then back to amos@taux01.nsc.com

---

**✂ re: You think YOU have problems with your telephone company?**

*laura halliday <halliday@vaou02.enet.dec.com>*

*Wed, 25 Apr 90 20:10:45 PDT*

The note in [Risks 9.83](#) about the Florida woman and her telephone 'service' sounded, remarkably like a failure I saw in a C-1 electronic exchange some years ago.

Background: the C-1 was a very early electronic exchange. It was a hybrid, with electromechanical line equipment and a digital computer for brains. The line equipment came in large cabinets, with cables to route calls from one cabinet to another and more cables for status information back to the processor.

The system went crazy one afternoon. You could pick up the phone and you would get dial tone perhaps 10% of the time. The rest of the time you'd get a mixture of other peoples' conversations, and busy and reorder signals. The phone would ring randomly, and you would get the same mixture of garbage if you answered it.

The problem turned out to be hardware. \*One\* wire had broken - one of those signal wires, and, since the line equipment cabinets were daisy-chained, and the broken wire was close to the processor, the whole thing went down. It was buried deep inside a cable run, and took a couple of days to find.

...laura halliday, DEC Canada, halliday@vaou02.enet.dec.com

Opinions: MINE! Nothing to do with DEC Canada.

---

**✂ re: You think YOU have problems with your telephone company?**

*<forags@nature.Berkeley.EDU>*

*Wed, 25 Apr 90 18:27:26 PDT*

Often when telephone installations are changed, not all wires which were connected to the original installation are disconnected. These residual connections can be in a central office, on a pole, or in a building. When a new phone installation re-uses these apparently "dead" wires, trouble can arise.

1. A friend found a modular telephone jack in the basement of a house which he just bought. The jack had dial tone, so he used it as an extension phone. A couple of months later, his neighbor remarked that he had been getting billed for long-distance calls which he had never made. My friend recognized the areas called as calls which he had made. Explanation: the former occupant of my friend's house had had two telephone numbers; the wire feeding the jack in the basement was connected outside on the telephone pole to the same pair as the neighbor's telephone.

2. My parents had their telephone number changed. They still got calls from

people dialing their old number. The service rep at the phone company said that was impossible -- the next call my parents got was from the service rep dialing their old number (she was very embarrassed, naturally). Apparently a jumper in the central office had not been disconnected so their phone rang through two separate numbers.

3. Many phones in my building at U.C. used to use 4-wire circuits. When we upgraded to 2-wire circuits (with the central office switch replacing a rack of relays in our basement), many of the extra wires were not disconnected from the telephones. I've traced three problems with new phone and data line installations to using pairs which were also connected somewhere else to a telephone although the wires were not used for dial tone.

Al Stangenberger, Dept. of Forestry & Resource Mgt., 145 Mulford Hall - Univ. of Calif., Berkeley, CA 94720 BITNET: FORAGS AT UCBVIOLE (415) 642-4424

---

**re: You think YOU have problems with your telephone company?**

*Pete McVay, TAY2-2/F14, 227-3598 <pmcvay%contra.DEC@src.dec.com>  
26 Apr 90 10:24*

I worked with a network security organization a few years ago. While my job did not directly involve phone phreak investigations (those individuals who attempt to hack "telecommunications" rather than "computers"), I did overhear some information that seems to fit in with the Kissimmee woman's phone problems--that is:

- o some hackers were known to have infiltrated major telephone networks and set up their own trapdoors and Trojan Horses in the switching software. The statement was made that "many telecommunications vendors are not in control of their own systems".
- o there was evidence that at least one phone phreak could do anything in a major phone system that the owners could--that is, grant services (call forwarding, etc.), disconnect or enable phone service, and change billing. This included the ability to make "invisible" (non-charged and unrecorded) long-distance phone calls.
- o some of this ability was used for harassment: law-enforcement officials and/or people the phone phreak personally did not like receive huge phone bills. Friends of phone phreaks found their bills greatly reduced.

The one item that does not fit, however, is the visibility of this woman's problems. Typically the phone phreaks kept their activities quiet: advertising them would spark an investigation and possible breakup of their access. Such harassment that did go on was minor and was not on a continuing scale such as this woman described. But maybe she antagonized a phone phreak in a major way: could she be a prominent community activist on social or environment issues, for example?

**re: You think YOU have problems with your telephone company?**

John Higdon <john@bovine.ati.com>

26 Apr 90 00:06:41 PDT (Thu)

Missing details in the mysterious case of the Florida woman experiencing much trouble with her telephone service make intelligent comment impossible. Probably most the most important consideration would be the type of central office switch involved. Since we are not dealing with an RBOC, it could be anything; some of those off-the-wall switches are capable of some rather bizzare behavior. Also, it is significant if this is rural service.

The "crossed line" problems sound like difficulties associated with "pair gain" equipment. To make an outdated, undersized outside plant serviceable, telcos sometimes resort to concentrators. These are devices that allow many subscribers to have what appear to be private lines over a somewhat smaller number of actual circuits. This is not to be confused with digital "remote" offices, which actually provide the functional equivalent of private lines (within their blocking factor limitations) over digital carrier back to the host central office. Concentrators are fraught with difficulty, most of it similar to the "crossed wire" effect observed by our subject.

All in all, it sounds as if our hapless woman is plagued with problems resulting from multiple causes: difficulty with the 800 carrier, possible CO trouble, possible outside plant trouble, etc. In my library of telephone experience, I have never had anything to compare with our Florida victim, but my universal solution might be something to consider.

On several occasions, I have had difficulty of one sort or another that the telco simply has not been able to correct. Either it has been of an intermittant nature and not detectable by test personel or the solution has just simply eluded the maintenance staff. When it appears that the difficulty cannot be corrected in a timely manner, I order a new service. After the new service is completely installed, the old (and troublesome) service is disconnected. This ensures that no part of the old service remains; not the cable pair, CO line equipment, nor any line conditioners or loop extenders. This tactic has not failed to correct seemingly "insoluble" problems.

Another consideration: if this woman is the victim of someone's maliciousness (a real possibility) then the solution might be elusive. This "someone" obviously has software (and most likely hardware) access to the telco and could be very hard to track down. A second, more likely but almost as difficult to deal with, possibility is that the telco is just plain messed up. In that case my "universal solution" might correct her current problems and bring on others.

In any event, I would be very interested in getting further details. If her area code/prefix could be revealed, I can determine what type of CO switch is involved. Also, I can probably research what type of outside plant we are dealing with. Solutions are not guaranteed, but the finger pointing might become a little more educated.

John Higdon, P. O. Box 7648, San Jose, CA 95150 +1 408 723 1395

## **re: You think YOU have problems with your telephone company?**

GREENY <MISS026@ECNCDC.BITNET>

Thu, 26 Apr 90 02:31 CST

Well, this may not be related to a phone company problem, but when I was an undergrad, the university decided to go from party line rotary phones, to a brand-spanking-new digital switch and give everyone their own private line.

No problem right? Well you know the answer to this one. Not only did we get our own phone lines, but all the neat features that come with a digital switch such as call forwarding, speed dial, three way call, call waiting, etc...And the ability to have a "secret" 5 digit code to bill your calls to.

Due to a "programming error" it was quickly discovered that you could use your "secret" code from any telephone on campus. And of course if you happened to incorrectly enter your "secret" code at another phone, chances were that it was someone else's "secret" code that you entered, and the call would go through! Of course when that person's bill came, it showed up as a call from a phone they weren't at for a number they didn't call. So of course the local telephone people on campus got this bug fixed -- after about a month and an unknown # of "misentered" secret codes...

After this fix, another neat thing would show up. During the late hours of the night (when all the CS hackers do their things and make avid use of all the modem lines on campus), the digital switch would tend to "hang", and would not produce a dial tone. Sometimes it would actually connect you as an additional party to a conversation in progress and although you could hear both sides of the conversation -- they couldn't hear you no matter what tone you sent or how loud you screamed. After the two parties hung up, if you stayed on the line, you would be connected to the next phone call which either of those two parties made -- although they could hear you this time. However they could not dial, and until you hung up they couldn't dial. Through some trial and error, a friend of mine and I discovered that by hitting \*99 (which would kill all of your personal speed dial #'s), that the entire switch would reset -- losing all the speed dial #'s, and other pre-programmed goodies...

Needless to say, after reporting this occurrence the university did nothing, so we talked to the makers of the switch -- GTE, and they came out and fixed it... No problems since then.

Moral of the story: Software controls our lives, and is written by people who are subject to sleeplessness, caffeine (or other drug addictions), or just plain forgetfulness (how many times have you left out a { in some C code?). We had all better be aware of the risks, and do the best we can...

Greeny BITNET: MISS026@ECNCDC



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

**Volume 9: Issue 85**

**Friday 27 April 1990**

## Contents

- [Computer error parks hundreds illegally](#)  
[Dave Harding](#)
- [Computers may be fattening?](#)  
[Gary Tom](#)
- [Unattended Plane Take-off](#)  
[Andrew Duane](#)
- [Aircraft electronics problems: A pilot's report](#)  
[Peter Ilieve](#)
- [1099 forms, risks, and technology](#)  
[Gregg TeHennepe](#)
- [Re: "It's a Computer Error"](#)  
[Pete Mellor](#)
- [Re: Risks of engine computers and EMP](#)  
[David Paul Hoyt](#)
- [Security Breach--cc:Mail Inc.](#)  
[Chris McDonald](#)
- [Queues and Servers](#)  
[Anthony E. Siegman](#)
- [Computers and names with special characters](#)  
[Lance Hoffman](#)
- [Computer Jammming of 911 LInes](#)  
[Gary McClelland](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✉ "Computer error parks hundreds illegally"

*Dave Harding* <[HARDING@MDTF08.FNAL.GOV](mailto:HARDING@MDTF08.FNAL.GOV)>

*Fri, 27 Apr 1990 12:16:24 CDT*

>From the Chicago Tribune, 25 April 1990

COMPUTER ERROR PARKS HUNDREDS ILLEGALLY

At least 1,000 Illinois residents outside the metropolitan Chicago area

were flabbergasted Tuesday when they received dunning letters from the City of Chicago for parking violations they didn't commit, according to police in several of the towns.

The Chicago Revenue Department mailed about 36,000 overdue parking notices, said John Holden, a Revenue Department spokesman. He said up to 10 percent of them could go to people who did not commit parking violations, most of them in the Quad Cities area.

Holden said the problem occurred because workers failed to differentiate the types of license plate numbers that are fed into the city's computerized system. The city contracts with Cumputil Inc, a New Jersey-based company, to feed license-plate numbers of overdue tickets into the computer, which automatically sends out notices to parking violators.

---

### **✂ Computers may be fattening?**

*garyt@cup.portal.com <Gary Tom>*

*Thu, 26-Apr-90 01:53:45 PDT*

>From the Health column of the April 25th San Jose Mercury News evening edition:

"Such modern conveniences as personal computers and extension phones could cause you to gain weight. Psychologist Thomas Wadden of the University of Pennsylvania attributes as much as seven pounds per year to using a computer rather than a typewriter. Keeping files stored in the computer means you don't burn calories getting up to fetch them. Ditto for extension phones, which save about 70 miles of walking a year, thus adding two pounds annually."

---

### **✂ Unattended Plane Take-off (Clive, RISKS.9.83)**

*Andrew Duane <duane@samsung.com>*

*Wed, 25 Apr 90 15:27:48 -0400*

This happened at a local (Lawrence, MA) municipal airport about 4 years ago. It seems that a pilot was prop-starting a small 4-passenger plane. The propeller spun, and the engine caught. The throttle must have been set, and the plane quickly took off, sans pilot. Luckily, it was also sans passengers. It got about 250 yards, then crashed into a nearby store.

On the evening news, the airport manager expressed his surprise, saying "this sort of thing rarely happens here."

I know, no computer risks, but it was relevant to the article.

Andrew L. Duane (JOT-7), Samsung Software America, 1 Corporate Drive  
Andover, MA. 01810 (508)-685-7200 X122

---

### **✂ Aircraft electronics problems: A pilot's report (from CHIRP in the UK)**

*Peter Ilieve <peter@memex.co.uk>*

*Fri, 27 Apr 90 09:18:30 BST*

This was reported in the Independent (a London paper) on 26 April. It is the pilot's account (abridged at one point) of the end of a flight from the Mediterranean to London. It was submitted to CHIRP, which is a reporting system run by the RAF Institute of Aviation Medicine to allow pilots to report anonymously on things that worry them.

"As we slowly descended through the stack, winds aloft were 70-80 knots with little or no turbulence. The Met continued to report strong surface winds but gave no warning of any exceptional turbulence.

"As we descended into the clouds, the situation deteriorated rapidly. The wind and turbulence quickly increased. At 3,000 feet inbound on the Instrument Landing System localiser we were experiencing westerly winds of 188 knots and we were encountering severe turbulence.

"When the first officer reported the wind to Air Traffic Control the reply was, 'Roger, understand Westerly 88 knots.'

"First officer: 'Negative, ONE-eighty-eight knots.'

"ATC: 'Good grief.'

"At about this time, the aircraft's automatics started running for cover. Both Flight Management Systems were repeatedly failing and recovering and at various times both autopilot and the captain's Flight Director (electronic artificial horizon) were out of action. The first officer was doing a great job in trying to round up the wayward systems while simultaneously monitoring my approach and handling.

"The ride down the Instrument Landing System was very wild with the wind indicating 150-180 knots. At 700 feet, with violent turbulence and an apparent 130 knots negative wind shear between that altitude and the ground we commenced a go-around.

"During the go-around virtually all the automatics failed again and the turbulence became extreme.

"Levelling at 3,000 feet, flaps and gear up but still in severe turbulence we were now confronted with further problems. Our 'bolt-holes' (diversion airports) began to look suspect. We determined only one diversion airfield was still just about okay, but now on the limit of our fuel reserves. We elected to go, and ATC started vectoring us through the traffic, at low level in heavy turbulence.

"At last we were cleared up out of the cloud and back into clear and relatively calm air. The automatics now started creeping out of the woodwork but we were still extremely busy, the two-crew operation really stretched to the limit.

"En route to the diversion, [we had to cope] with a combination of failed automatics, unfamiliar ATC clearances, monitoring the weather, to say nothing of liaison with the cabin crew, and the very frightened passengers. We had about 30 minutes fuel available and we *\*had\** to make it in, and with the weather deteriorating literally by the minute it had to be the first time."

The Independent piece goes on to link this with the completed but as yet unpublished report on the 737 crash at Kegworth, which is believed to be critical of the design of electronic cockpits, and also reports from British Airways of 6 incidents with their new 747-400s. In each of these, the automatic systems closed all 4 throttles while the aircraft were climbing. A previous report in the paper had suggested some sort of sensor

problem, I think concerning the flaps, as a cause of this problem

Peter Ilieve peter@memex.co.uk

---

✦ **1099 forms, risks, and technology (Karn, [RISKS-9.81](#))**

<gateh@CONNCOLL.BITNET>

Thu, 19 Apr 90 12:05:49 EDT

Phil R. Karn (karn@thumper.bellcore.com) writes:

- > One wonders if there may be a fundamental limit on the degree to which
- > institutions that must be open to many sources of public input can rely
- > on a high degree of computerization to achieve cost-effectiveness,
- > especially when the institution or its policies are unpopular.

While sociologists/psychologists might argue that, based on certain predictable human traits, there will but such a limit, I am inclined to disagree. It seems to me there are two basic approaches for dealing with risks:

- modify/control the surrounding environment via automated systems, etc. in such a way as to reduce the risk posed to humans
- modify/improve human skill and intelligence such that the surrounding environment poses as little risk as possible

If one takes the first approach and assumes a basic level of human carelessness (both in the sense of error and in the sense of maleficence, as in the case of the 1099 forms), and tries to compensate for or insulate from risk via external controls, there will be such a limit, and it will be governed by the integrity of those controls. If on the other hand one attempts to reduce error and maleficence via internal control (human education/training/self-discipline), the limit will be governed by the human potential.

It seems to me that ideally what is needed is a combination of these two approaches. My fear is that presently many if not most systems are designed with the assumption that the human operator is a worst case, and so these systems provide little if any motivation/reinforcement for improving the human. To approach the problem of the limit of the utility of a particular technology by saying, Well, I guess we need to refine, we need bigger, better, faster is IMHO a mistake in that it is in some sense self-destructive. It tends to remove responsibility from the human, and as such allows and possibly encourages the atrophy of human skill and intelligence.

For me, this is what I think life is all about: impeccability is the task of living, and should begin with the person. From there it will move to the things created or maintained by the person. Unfortunately I don't think it works in reverse (ie. an impeccable system begets a better user). As a result I am somewhat leery of any system which takes control away from me, especially in light of the fact that I often have no way of knowing the integrity of either the system or its designer, not to mention that it is likely the system was designed with an idiot in mind.

Gregg TeHennepe, Minicomputer Specialist, Connecticut College, New London, CT

---

**Re: "It's a Computer Error" ([RISKS-9.82](#))**

*Pete Mellor <pm@cs.city.ac.uk>*

*Wed, 25 Apr 90 22:48:55 PDT*

> I have noticed a recent upsurge in UK news reports of "Computer Errors".  
> Not of the major catastrophe kind, but of the "bill for \$0.00" sort  
> This seems to be intimately related to the introduction of the Poll tax.

Note for non-UK readers: What is euphemistically described by the government as the "Community Charge", and by everyone else is called the "poll tax" ("poll" as in "head": the idea that paying the tax is connected with the right to vote is a popular misconception) came into force in England and Wales in April this year. (Like many other things, it was tried out in Scotland first.)

In a nutshell, the previous system of "rates", an annual charge which was geared to the value of an individual's real estate, and which provided part of the funding for local government services (drains, emptying dustbins {sorry! garbage collection :-}, etc.) has been replaced with an annual per capita charge. Under the previous system, Lord Muck in his castle paid through the nose, while Joe Public in his two-up/two-down paid comparatively little. Under the new scheme, Lord Muck and Joe Public pay the same. Joe Public is not too pleased about it. So unpleased about it, in fact, that on 31st March a demonstration in central London against the poll tax turned into a very ugly riot.

> I wonder if any other RISKS subscribers have noticed this phenomenon  
> (not the poll tax, the computer errors) ?

Try this one (Andrew Moncur's Diary column, Guardian, 4th April). I quote:

"If any rioting breaks out in Tunbridge Wells you shouldn't be too surprised to see Amy Mercer somewhere in the background, making a great deal of noise. She's just received her poll tax demand (&322-odd to pay). All very well. Except that Amy is eight months old - and, I would guess, fairly militant."

It will not surprise RISKS subscribers to learn that the changeover involves a *\*massive\** bureaucratic exercise, registering, and sending demands to, every person in the country over a certain age. Hardly surprising that someone thought it might be a good idea to use computers to help with the work.

Presumably, these same computers will also be used to record people who do not pay, and trigger the various steps taken to recover payment. (Not *\*registering\** is a criminal offence. Not *\*paying\** is a civil matter between the individual and the local authority, who must take each individual case through a procedure of which the final step is the magistrates' court.)

Huge and well-organised campaigns of non-payment are under way.

Peter Mellor, Centre for Software Reliability, City University,  
Northampton Square, London EC1V 0HB Tel.: +44 (0)1-253-4399 Ext. 4162/3/1

---

**✉ Re: Risks of engine computers and EMP (Grant, [RISKS-9.83](#))**

*david paul hoyt <YZE6041@vx.acs.umn.edu>*

*Thu, 26 Apr 90 09:18 CDT*

> ... it would also kill the engine computers in every late model car.

Actually it will stop and probably distroy all old cars too. An EMP will arc the points and fuse the alternator. Everything looks like an antenna to an EMP blast.

---

**✉ Security Breach--cc:Mail Inc**

*Chris McDonald ASQNC-TWS-RA <cmcdonal@wsmr-emh10.army.mil>*

*Wed, 25 Apr 90 12:20:26 MDT*

>From "MacWEEK", 24 April 1990:

"In respoonse to a breach of its E-mail system's security, cc:Mail Inc. this month will ship a new version of cc:Mail free to all users. The upgrade offers enhanced security to combat an unauthorized utility that lets users access other users' mail.

Posted on a Hayes Microcomputer Products bulletin board by an unknown source, the utility lets a user gain access to all cc:Mail passwords and messages on a LAN.

cc:Mail has notified all it customers by phone or e-mail about the security breach and has set up aspecial tool-free hot line at (800)338-9012.

Previously unregistered cc:Mail customers are also eligible to receive the free upgrade."

---

**✉ Queues and Servers (Re: [RISKS DIGEST 9.82](#))**

*Anthony E. Siegman <siegman@sierra.Stanford.EDU>*

*Wed, 25 Apr 90 13:13:24 PDT*

Careful. Didn't Scientific American have a fascinating story on task scheduling a few years ago pointing out that there are nonpathological situations involving a single queue of variable-length tasks and multiple servers, IN WHICH ADDING AN ADDITIONAL SERVER CAN ACTUALLY MAKE IT TAKE LONGER TO FINISH THE QUEUE?

[Yes, VERY OLD RESULTS, originally from Ron Graham and Vic Benes (when I was at Bell Labs in the 60s, if I recall correctly), for nonstochastic

queues. See Coffmann and Denning, Operating Systems Theory, Prentice-Hall, 1973, in which some of Ron Graham's examples reappear... A wonderful family of cases in multiple dimensions, where apparent simplifications in any one dimension can actually make things worse. PGN]

---

## ✂ Computers and names with special characters

*lance hoffman <hoffman@gwusun.gwu.edu>*

*Wed, 25 Apr 90 14:08:12 EDT*

Following up on the contribution regarding hyphenated last names at the Social Security Administration, when I did some consulting there years ago, we were told of the incident where one person who was receiving checks insisted on changing his surname to something like "\*N" (not his real name). You can imagine the havoc this caused until the agency went and implemented something like 25 patches in 25 different systems, which they did, on the humane grounds that you can call yourself whatever you damn well please.

Professor Lance J. Hoffman, Department of Electrical Engineering and Computer Science, The George Washington University Washington, D. C. 20052 (202)994-4955

[It really opens up some possibilities, including VictorBorge-style pronunciations of nonalphabetic characters. PGN]

---

## ✂ Computer Jammimg of 911 Lines

*"Gary McClelland" <gmcclella@clipr.colorado.edu>*

*26 Apr 90 10:37:00 MDT*

The Boulder [CO] Daily Camera (25 April 1990) reported that local police have arrested a suspect in the jamming of police communications and the 911 system. According to the article, he used radio devices to jam the police radio frequencies and a computer to interfere with the 911 lines. The newspaper article gave no details on how he used the computer to jam 911 system. Since the local 911 system has ANI and it took the police a while to find the guy, he presumably was doing something more sophisticated than just making multiple calls to 911 with his modem. No reports of any emergencies that received delayed attention because of the jamming.

The motive: The University of Colorado campus police issued this guy a warning citation (no fine) for failing to leave the physics building during a fire alarm test. He then started messing with the campus police communications and then moved on to harass the city police and jam 911. Makes you worry about what he will do now that they have arrested him and made him really mad!

Gary McClelland, Univ of Colorado



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

**Volume 9: Issue 86**

**Monday 30 April 1990**

## Contents

- [Futures market shut down](#)  
[Steve Bellovin](#)
- [Habsheim A320 crash](#)  
[Clive Feather](#)
- [Throttle Hitch Hits 747-400](#)  
[Robert Dorsett](#)
- [Re: Unattended Plane Take-off](#)  
[Jan I Wolitzky](#)
- [Re: Computers and names with special characters](#)  
[Mike Van Pelt](#)
- [Inadequate documentation - truncated GPAs](#)  
[Doug Sewell](#)
- ["The return of the hacker"](#)  
[David B. Benson](#)
- [Indian Professors Teaching Virus Writing](#)  
[Cliff Stoll](#)
- [\(Not necessarily\) computer parks hundreds of cars illegally](#)  
[Bill Gunshannon](#)
- [Info on RISKS \(comp.risks\)](#)

---

### futures market shut down

<[smb@ulysses.att.com](mailto:smb@ulysses.att.com)>

Fri, 27 Apr 90 13:43:58 EDT

Five New York futures markets went off the air Friday when the communications line that delivers price quotes to brokers and others around the country failed. The cause of the failure is unclear as of this writing; exchange officials blamed AT&T lines, but AT&T said that their lines were working and that the problem appeared to be at the futures exchange.

And the traders -- most of them headed for home, a decision perhaps eased by the fact that the weather here is gorgeous and it's Friday...

--Steve Bellovin

## ✂ Habsheim A320 crash

Clive Feather <clive@ixi.UUCP>

Fri, 27 Apr 90 09:18:50 bst

Another article about the A320 Habsheim crash appeared in the 11-17 April 1990 issue of Flight International. This includes transcripts of the voice and data recorders of the flight.

Time: seconds part of time; times are from 12:44:27 to 12:45:41.5.

N1: engine low-pressure compression ratio (%)  
(a good guide to engine power).

CAS: calibrated air speed, in knots.

V:

A = radio altimeter (heights are in feet)

C = captain

G = ground proximity warning system (GPWS)

N = noises

P = copilot

T = tower

N1 and CAS values are interpolated from a graph in the article. This only covers the time from 12:45:00 to 12:45:39.

Time N1 CAS V

27 T QNH Habsheim 1012 Fox Echo 984.

C OK.

[QNH is the altimeter pressure setting required to make the altimeter read 0 at sea level ("altitude"), and QFE is the setting to make it read 0 at airport ground level ("height").]

31 P Roger. [On radio]

32 C 984 put in 984.

34 P 984 QFE selected.

37 P Good gear is down; flaps 2.

42 C Flaps 3.

45 P Flaps 3.

C That's the airfield; you confirm ?

48 P Affirmative.

51 P You see it LL01, when we get there you're at 1 nautical mile, that's right.

55 N <Gong> [nosewheel valve, according to crew]

P OK.

G Too low terrain.

00 35 160

04.7 N <Gong> [GPWS cutoff, according to crew]

05 35 150

05.7 A Two hundred.

10 35 150

11 P P...G...

[P...G... is the airline's flight safety officer]

11.4 A Two hundred.

12 P G.... is going to ... eh.  
 14 P OK, you're at 100 feet there, watch, watch.  
 15 35 145  
 15.3 A One hundred.  
 19.1 A Forty.  
 20 35 135  
 23.6 A Fifty.  
 25 35 130  
 26 C OK, I'm OK there, disconnect autothrottle.  
 [This had already been done].  
 27.5 A Forty.  
 30 35 120  
 32 P Watch out for the pylons ahead, eh, see them ?  
 33 C Yeah, yeah, don't worry.  
 34 35 [Throttle position started moving from 0 degrees]  
 34.5 35 N <Clack, clack, clack> [power lever detents]  
 35 35 115  
 35.3 A Thirty.  
 36 38 [Throttle position reached 45 degrees, where it then remained]  
 36.2 A Thirty.  
 37 45 P TOGA/SRS. [Take-off go-around / speed reference system]  
 38 60  
 38.3 A Thirty.  
 39 75 100 P Go around track.  
 N <Increase in engine speed>  
 N <Noises of impact in trees>  
 39.9 C Sh..!  
 41.5 END OF TAPE

Some other notes from the article:

Air France's approved overfly height is 100 feet, and only if the runway is suitable for landing. Habsheim's runways are too short to land an A320.

The original plan was to overfly the hard runway, 02. The captain was clearly having trouble finding the runway; when he finally saw the line of spectators on the ground, he decided to overfly the grass runway 34R, without telling the copilot.

The captain was used to major airports, with 2000-3000m runways and 30m high control towers. Habsheim has a 800m grass strip and a 12m high tower. He may have been misled by a scale effect; the steep attitude of the plane would have enhanced this, and could also have made him think he was higher than the trees (which first struck the rear fuselage).

It was suggested on RISKS that there may have been a software delay in the engine controls which was not shown by the data recorder. From the voice tape, it is clear that this is not the case. A CFM56-5 engine takes about 8 seconds to spool up to full power, and the tapes are also consistent with this. N1 started to increase within half a second of TOGA (take-off go-around) power being selected, and had reached 85% when the engines began to ingest branches. Analysis of the soundtrack of a video shot from the control tower agrees with this, and shows N1 reaching 91% with "massive ingestion of branches and leaves".

Somewhere around 12:45:39 the captain's sidestick was pulled to full climb position. At this point the CAS was 110 knots, beginning to respond to engine thrust, and the height is 30 feet, steady and beginning to increase. Throttles and sticks are hard against the stops.

The first data recorder transcription suffered a misreading in the region 12:45:24 to 12:45:32, of which 4 seconds was rejected by the data checking software in the analyser. An example of errors produced was sign inversion of the aileron positions. The official report states that this "was no doubt due to an interruption of contact between the reading head and the recorded tape, caused by a fold in the tape and/or dust. The following recordings, made after cleaning and smoothing out of the tape, permitted correct reproduction of all data". This problem has been used as grounds for alleging that the data was tampered with, but it should be noted that (a) the affected area does not cover any significant events, and (b) the final transcription is internally consistent, and is consistent with videos taken by various people and air traffic control tapes. The voice recorder analysis was made with the crew's help.

Habsheim weather at 12:50:

wind 330/6 knots;

visibility 8km;

cloud 1/8 Cu at 780m, 7/8 Sc at 1500m.

The weather was unchanged since 12:20, except that the wind direction had backed from 010.

Clive D.W. Feather, IXI Limited, 62-74 Burleigh Street, Cambridge U.K. CB1 10J

---

### **✈ Throttle Hitch Hits 747-400**

*Robert Dorsett <rd@walt.cc.utexas.edu>*

*Fri, 27 Apr 90 16:27:51 -0500*

>From FLIGHT INTERNATIONAL, April 11, 1990:

``British Airways (BA) Boeing 747-400's have experienced uncommanded inflight closure of all four throttles on six separate flights between 6 October, 1989, and 19 February, "several times" on one of these flights alone, according to formal reports. Several other airlines have suffered the same incident, Northwest reporting it first.

``Boeing believes that it has determined the cause, and appropriate auto-throttle software modifications were made available to operators on 22 February. Initial modifications to all new aircraft were reviewed in early September. Studies continue, however, in association with airlines and the UK Civil Aviation Authority.

``Boeing and BA deny reports of serious unreliability, associated mainly with the 747-400's digital cockpit avionics and computerised systems management. Boeing reports world fleet technical dispatch average in 1990 as 94.5%, and gives a February 1991 target of 98%. BA says that its fleet of seven achieved

100% technical dispatch reliability in the last week of March, and 96.5% for the last three months, quoting this as reasonable for a new type. In most of the events the power levers retarded rapidly to idle, but sometimes the reduction was partial, followed by automatic reset. Pilots reacted by disengaging the autothrottle and resetting power manually.

``Boeing began a study of the problem as soon as reports confirmed that a throttle closure on a Northwest 747-400 was not a freak event. The manufacturer subsequently issued two service bulletins to -400 operators.

``All incidents have occurred in the climb or cruise, and an indicated airspeed (IAS) of more than 280 kt is believed to be fundamental to the event. If continuing experience confirms this, it means that stalling--even clean--is not a risk. Evidence indicates that the event is caused by a spurious signal to the full-authority digital engine control from the stall-management module. The "single word" spurious command says that the undercarriage is down or the flaps are at setting 1, so if the IAS exceeds the maximum speed for these configurations, the autothrottles close to reduce IAS to limiting speed, then reset to maintain it.

``The modification assumes that the fault was in the processing logic of the appropriate universal logic card (a printed-circuit software unit), and adopts a standard technique for reducing digital oversensitivity: there is now a delay (a few microseconds) built into the software by requiring it to receive an "eight-word" command before acting. Power spikes or other spurious commands should not produce a reaction.

``So far the latest modification has proved effective. Early corrections, though, had assumed the reaction was associated only with main-gear selection, so although software changes had reduced the incident rate, spurious flap signals continued to set engines to idle. BA has not reported any further events since February."

Robert Dorsett, Moderator, Aeronautics Mailing List

---

## ✂ Re: Unattended Plane Take-off

*Jan I Wolitzky <wolit@att.com>*

*Mon, 30 Apr 90 09:33:53 EDT*

It's not a passenger-carrying plane, but Boeing's new Condor unmanned (note sexist language) aerial vehicle (UAV) should be of interest to readers of this newsgroup.

The Condor is a 10-ton, 200-ft wingspan (greater than that of a 747), high-altitude (66,908 ft), long-duration (2.5 days), twin-engine, piston-powered, autonomous (NOT remotely-piloted) plane. Boeing hopes to find buyers in the military and scientific communities interested in the plane as a sensor platform, at \$20 million a pop, not including payload. DARPA has funded some of the development.

The plane is "piloted" by two Delco Magic 3 flight control computers, using

inertial guidance for navigation, a microwave landing system (MLS) for takeoff and landing, and about 60,000 lines of code, mostly Fortran, with some assembly code.

"All of Condor's mission functions from takeoff to landing are stored in its computers at the start of a mission...  
Communication links are provided so that the mission program can be altered in flight if necessary for safety or any other reason."

It operates autonomously within the air traffic control system (a contradiction in terms, as I see it), which has caused some concern on the part of the FAA. At its cruising altitude, it operates well above commercial traffic, but it takes 4 to 6 hours to get up there or back down. During flight tests, a chase plane was present whenever the Condor was within an airport traffic pattern. The article I read (*Aviation Week & Space Technology*, 132/6, April 23, 1990, pp. 36 - 38) had no word on what the chase plane's pilot's instruction were in the event of a computer malfunction, or what would happen if something failed when the chase plane wasn't around.

Jan Wolitzky, AT&T Bell Labs, Murray Hill, NJ; 201 582-2998  
(Affiliation given for identification purposes only)

---

### **✂ Re: Computers and names with special characters (Hoffman, [RISKS-9.85](#))**

*Mike Van Pelt <mvp@hsv3.UUCP>  
27 Apr 90 23:54:11 GMT*

Now that has some interesting possibilites -- If the Social Security Administration still uses Univac/Sperry/Unisys computers, I ought to change my name to @FIN (the end-of-job control card). That would sure drop a large monkey wrench into the works, as there is no way to read a card that starts with those four characters. Well, maybe if you switch the card reader translation mode to EBCDIC or column binary... (Assuming they still use cards, of course, which wouldn't surprise me at all.)

There are, of course, other variations if they've switched computers.

Mike Van Pelt, Headland Technology,

---

### **✂ inadequate documentation - truncated GPAs**

*"Doug Sewell" <DOUG@YSUB.BITNET>  
Sat, 28 Apr 90 13:02:08 EDT*

Several years ago, we split our report-card-printing job into two jobs. Due to the way it was split, one program was 'cloned', rather than modified to determine which set of report cards was to be printed.

The fact the both programs had to be kept 'in sync' wasn't clear in the documentation. I suspect that the interface between some of the

other procedures involved were also under-documented.

Some time after the job was split into two, the university got flooded with calls complaining that some of the GPAs were truncated - 3.95 and 3.13 were both printed as 3.00. The correct GPA could be determined by dividing the quality points by the hours attempted, which were both printed correctly on the report cards.

Apparently, some program maintenance affected the two clone programs. One printed GPAs correctly, the other didn't. During analysis, it was determined that the database files were correct, the permanent record reports were correct, and it was only half of the report cards that were printed incorrectly. It was necessary to reprint and remail all of the report cards.

Doug Sewell, Tech Support, Computer Center, Youngstown State University,  
Youngstown, OH 44555

---

### **✂ The return of the hacker**

*David B. Benson <dbenson@cs2.cs.wsu.edu>  
Sat, 28 Apr 90 11:43:50 pdt*

I have been throughly enjoying reading

Darrel Ince  
Software Development: Fashioning the Baroque  
Oxford University Press, 1988  
ISBN 0-19-853757-3  
ISBN 0-19-853758-1 (Pbk.)

which includes a chapter entitled "The return of the hacker". The particular risks discussed in this chapter and of immediate interest are in the use of spreadsheets by the computer less-than-adequately-literate.

When I mentioned computerized spreadsheets to some of my colleagues, they replied with some stories involving incorrect spreadsheet packages and also more stories of the hacking which occurs in the spreadsheet community.

While the misuse of spreadsheets may be less dramatic than problems with airplanes and autos, I suspect this spreadsheet hacking may be so pervasive as to have a noticable and negative impact upon the economies of the computerized world. (Of course, the widespread and judicious use of spreadsheet packages certainly has a noticable and positive effect as well. But on RISKS we concentrate upon the negative impacts.)

I would appreciate the readership of RISKS contributing a wide variety of stories about spreadsheets. These might include stories about the incorrect implimentations of constraint programming which appears to occur in all-too-many of the spreadsheet packages. These stories would also ideally be about the real-world impacts of trusting the conclusions obtained by the spreadsheet packages. (If you haven't any stories of your own, please just ask the tradespeople in the community in which you reside.)

---

## ✦ Indian Professors Teaching Virus Writing

Cliff Stoll <cliff@cfa253.harvard.edu>

Mon, 30 Apr 90 01:59:14 EDT

This from News Notes on America-On-Line, April 28, 1990:

### Seminar Speaker Says India Should Pass Anti-Virus Legislation

Those attending a seminar last week in New Delhi urged the Indian government to consider a law to deter people from indiscriminately experimenting with viruses. A report in the Xinhua Chinese news service quoted an Indian scholar identified only as "Mahabala, chairman of the department of electronics committee on computer virus" as saying an alarming trend in the country is that some academics are teaching software engineering by creating viruses for their students to detect. Said Xinhua, "This concept of glorifying viruses designers (is) wholly destructive," adding Mahabala cited a wide variety of viruses affecting computers in India, mainly variations of viruses such as "C-Brain." Mahabala said that, instead of creating viruses as means of copy protection, software designers should come out with access passwords that are difficult to break.

--Cliff Stoll cliff@cfa.harvard.edu

---

## ✦ (Not necessarily) computer parks hundreds of cars illegally

bill gunshannon <702WFG@SCRVMSYS.BITNET>

Mon, 30 Apr 90 08:21:05 EST

Although this looks like a computer/operator glitch up front, it could also be an example of using the old? cliché "computer error" to cover up some shady fund raising. There was a case a number of years ago when Philadelphia sent out thousands of parking tickets also to people who had not even been in the city. The idea being if even 1% send in the money rather than fight the ticket, they show a handsome profit. My father received one and took it to the local AAA office. They were taking them to Harrisburg by the hundreds just from the NE PA area. Of course, they didn't have computers to blame so uncovering the scam was pretty easy.

It seems that computers may be capable of providing a good audit trail when desired but they are also capable of covering their tracks if that is the desired result.

bill gunshannon



Search RISKS using [swish-e](#)

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





Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

**Volume 9: Issue 87**

**Tuesday 1 May 1990**

## Contents

- [Phones & techologically illiterate operators](#)  
[David A. Honig](#)
- [More telephone problems -- union pressures](#)  
[Peter Jones](#)
- [Forwarding: Weird phone bills - an unexplored possibility](#)  
[Chaz Heritage via Richard Busch](#)
- [Re: Call Forwarding](#)  
[Peter Jones](#)
- [Kissimmee Kate](#)  
[Geoffrey H. Cooper](#)
- [Re: You think YOU have problems with your telephone company?](#)  
[Gary Cattarin](#)  
[Jozsef A Toth](#)  
[Warren Levy](#)
- [Blaming it on the computer?](#)  
[Brad Templeton](#)
- [Re: Risky McDonald's comrade...](#)  
[Charles Youman](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **✉ Phones & techologically illiterate operators**

*"David A. Honig" <[honig@BONNIE.ICS.UCI.EDU](mailto:honig@BONNIE.ICS.UCI.EDU)>  
Thu, 26 Apr 90 12:40:20 -0700*

This is unrelated to the recent discussion of central office problems,  
but definitely a computer-related phone RISK.

I tried to get an operator to make an emergency break-in to a friend's line  
which was busy. She reported that the line was out of order, and could not  
break in.

I found out that he had been using a modem. The hapless operator must have  
listened in (prior to interrupting and asking if the emergency break-in should

be obeyed) and heard 1200 bd screeching. To her, any non-voice signal must have meant "out of order". Of course, it wouldn't have helped to try to break in to the "conversation", unless she could whistle real fast. :-)

If she had told me that she heard "telecommunications" or something, I would have logged in myself and located my friend on the computers...

---

**✂ More telephone problems -- union pressures (Re: [RISKS-9.84](#))**

*Peter Jones <MAINT@UQAM.bitnet>*

*Thu, 26 Apr 90 16:57:13 EDT*

In the Universite du Quebec a Montreal, where I work, the employees' union used the call forwarding feature in a pressure tactic several years ago. Employees participating employees forwarded calls at random. Callers got busy signals and of course many wrong numbers. At that time, calls could be forwarded to outside numbers; people calling the university ended up at radio stations, at newspapers or elsewhere. Since that incident, call forwarding to the outside is only allowed by special permission of the telecommunications department.

This is not so much an example of technology gone wrong, but rather of people using it for political purposes.

Another political example I remember is the spiffy direct-dial international service that was in operation in Moscow during the Olympics (can't remember which ones). The system was dismantled afterward because the KGB couldn't keep up with the volume of calls (I wonder if this is an authentic story, or just a joke.)

Peter Jones (514)-987-3542

---

**✂ Forwarding: Weird phone bills - an unexplored possibility**

*<"Richard\_Busch.SD"@Xerox.COM>*

*26 Apr 90 18:52:30 PDT (Thursday)*

Date: 26-April-90 (Thursday) 4:20:38 PDT

From: chaz heritage:wgc1:RX

Subject: Weird phone bills - an unexplored possibility

To: Richard Busch

>These troubles with the phone company have resulted in huge bills for calls that apparently were never made...It's only a software problem?<

While I don't doubt that a software fault could have caused the complainant's problems, and wouldn't read RISKS if I didn't think that such faults should be investigated by folks like PGN, there is a possibility that no technical fault is involved.

[I should have had quotes around "It's only a software problem?". This was intended to be reminiscent of the old SMOP yarns, "It's a Small

Matter of Programming". PGN]

Over the last ten years a number of public monopolies in Britain have been 'privatised' - sold to the private sector by the Government. One of them was British Telecom. A 'competing' company, Mercury, was also set up, but for technical reasons domestic and small business subscribers are now dealing for their phone services with a single private monopoly.

A catalogue of the new British Telecom's crimes would exceed reasonable bandwidth, but one noticeable trend seems to be the issuing of phone bills for slightly unreasonable amounts, in the hope that people might simply pay the bill without checking it (not all subscribers are willing to pay extra for an itemised bill). Business subscribers seem particularly prone to this. At home we have had to query every bill sent to us since privatisation; the last one was for #44,000! Others involve fairly small additions, however; three international calls here, a number of unusual operator services there, and so forth.

Could it be that the phone company involved in PGN's case are simply trying it on in the same way? Since everyone is so concerned over 'computer errors', it is easy to blame the unfortunate silicon idiot for everything. The unscrupulous might see an opportunity here. Perhaps the willingness of people to accept 'computer error' as an excuse for what might well be deliberate is a RISK in itself.

Chaz

---

**✂ Re: Call Forwarding (Novick, [RISKS-9.84](#))**

*Peter Jones <MAINT@UQAM.bitnet>  
Thu, 26 Apr 90 16:24:24 EDT*

In Montreal, and possibly in all of Bell Canada's territory (Quebec and Ontario), the phone rings briefly to notify the subscriber that a call has been forwarded. Thus, the subscriber is reminded to cancel Call Forwarding when he's home and a call comes in.

Note: If a subscriber has Call Waiting, and forwards to himself, the caller gets a busy signal instead of a ringback, and the call in progress is not disturbed at all. Very useful when a data call is in progress, for our system doesn't allow the subscriber to temporarily disable Call Waiting, except in certain areas. When the phone is back on hook, the brief ring mentioned above is heard, the caller gets a busy signal and incoming calls cannot be answered until Call Forwarding is cancelled. (I've been told this, but have never tried it myself.)

Some systems automatically make a call to the forwarding number when forwarding is requested. This makes it possible to check the number is working, and is the right one. The disadvantage is the incurring of a possible toll charge.

Peter Jones UUCP: ...psuvax1!uqam.bitnet!maint (514)-987-3542

---

**Kissimmee Kate**

*Geoffrey H. Cooper <geof@aurora.com>*

*Fri, 27 Apr 90 11:18:33 PDT*

I have two inputs, one is pretty related and one is a bit further away. I remember Jerry Saltzer talking about a problem in his home with an amazing number of wrong number calls received. These were ultimately traced down to a bad connection in a crossbar switch. One entry on the crossbar was connected to a busy signal or message. Calls from other central offices were routed to that connection if the destination was busy. It happened that Jerry's home number was connected adjacent to this "busy-signal" entry, which ultimately turned out to have a bad contact or relay. The result was that all busy calls from outside the local office were converted into misrouted calls to the Saltzer residence. Jerry can probably give you a better description of what it was (my memory is somewhat hazy).

The other bug is not a phone bug, but it fell into consciousness because it had the same kind of random delaying action you mentioned. I hope it is more of a help than a distraction.

> ... not understanding how he reached the Yellow Cab company when [about  
> three minutes later] the telephone rang and [the officer] answered the phone  
> only to be connected to a Howie, a dispatcher at the police department,

About 1981 or 1982 at MIT, Dave P. Reed (now at lotus) and I were perusing the code that was then used for TCP-IP under Twenex (all that code was subsequently replaced). I had seen astonishing packet delays when Twenex was used as a gateway. In one case, a packet was delayed for about 5 minutes. I only detected it because I had forgotten to turn off "etherwatch" while I got ready to leave the office. As I walked over to logout of the Alto, the final packet of 10 arrived magically.

My recollection is that the software had a kernel task with an input queue that processed each packet by doing some simple processing and enqueuing it to the next task. The assembly code was in the form of:

```
more_packets:  
  process first packet  
  *goto more_packets  
  deschedule task
```

The assembly line with the \* was inadvertantly omitted, so only one input packet was being processed for every time the task was scheduled. Thus in the rare case that two packets were both in the queue, the second would be delayed until the next packet that arrived at the interface, which could be arbitrarily later.

I don't recall why the software didn't eventually end up with all the packets in that queue -- but it was pretty buggy software, so maybe

something like that did happen eventually.

Relationship to phone hacking...

What if the "call parking" feature is just a special case of the way calls are always made, such that a queue exists that causes a call to be placed when the line is free. All calls are put into the queue, and a flag on the subscriber line or queue entry indicates whether to flush the attempt if the user doesn't wish to park the call.

In this case, a subtle modification of the system code or even a hand-patched queue entry could sit in the queue for an arbitrary amount of time. Similarly, a daemon could queue calls randomly.

Just speculation.

- geof

---

### **✂ Re: You think YOU have problems with your telephone company?**

*<Gary\_Cattarin@DG\_SUPPORT.MCEO.DG.COM>*

*Fri, 27 Apr 90 07:50:48 edt*

CEO summary:

Owing to the vaguaries of the mail system, I never saw the Tale of Kissimmee, though I bet I'll get it in a month or two... The reactionary tales of 9.84 certainly rang a few bells, to coin a pun.

Back in my undergrad days, my university (RPI) also decided to go winto the phone business. They bought an Intecom switch (I think) and were promptly christened "Tute Bell" after the school's nickname.

This switch had a unique feature. You couldn't forward your phone to your own phone DIRECTLY, such as "forward to 5555", but you could do so via an outside line, such as "forward to 9-266-5555. You could then call yourself via an outside line, and the system would promptly forward your call back out from the switch to the phone company who'd send it back, where, guess what...it would happen again. Each out-and-back loop used two trunk lines, and this would go on indefinitely. Each time the call came back through your phone, the phone would emit a short ring, telling you that two more lines were tied up. Although we never did it (honest!) we figured it would be quite easy to cripple the institute by tying up all the lines, or at least crash the switch. All this from one phone!

---

### **✂ RE: You think YOU have problems with your telephone company?**

*Jozsef A Toth <jatst3@unix.cis.pitt.edu>*

*Fri, 27 Apr 90 15:42:36 -0400*

I had a similar problem a couple of years ago. My long distance carrier was (and still is) US Sprint (lowest prices around!) At any rate, I was in the

midst of moving, but still wanted a US Sprint calling card. US Sprint would not grant me a card without a home telephone number, so I used my sister's phone number/address until I settled into a new place (which would have a phone), the delta time between old place and new place was 45 days. Once I settled into the new place, I was set up with US Sprint "Dial 1" service and an accompanying Calling Card. Therefore, I stopped using the card associated with my sister's address/phone and commenced using the new one.

Six months later, I moved a second time to a new address, and you guessed it, a new phone. I signed up for US Sprint "Dial 1" service and an accompanying Calling Card. Again, I stopped using the card associated with the previous number. At this point, I had three US Sprint calling card accounts but I was only using the most recent one. US Sprint customer service assured me that my "accounts had been consolidated" and that all my calls would appear on one bill, associated with my current address/phone number. Just for grins, I think (I'm not sure if this was exhaustive) I tried the two old calling card access codes, and I was rejected.

This was late '86, early '87 and all took place in the 412 area code, the greater Pittsburgh area. Please be patient, I'm setting the stage as accurately as I can. In June/July of '87, my sister moved to San Fran w/ her husband. Their long distance carrier was AT&T or MCI (can't remember.) Remember when I originally signed up with her phone for a US Sprint Card? I only used her address/phone as a security blanket for the US Sprint billing people, she still had another Long Distance carrier and I specified the billing address, which can be different from the reference phone/address.

After my sister moved, I started to receive calls to Fort Lauderdale FL on my monthly US Sprint bill. To boot, some of them were person-to-person collect to my Sister's old number. SO I called the number that used to be my sister's and spoke with the new owner of that number. They were making/receiving collect calls from Fort Lauderdale, FL. and they were being billed for them, and at the same time, SO WAS I!

Next came the endless calls with Customer Service, Xerox copies of my phone bills mailed to account managers, their boss and their boss' boss, etc. Around this time, I had read that US Sprint was in a lot of red ink because of their antiquated billing software (US Sprint was purchased from someone else, can't remember the name). All the people I talked to at US Sprint insisted that there was nothing wrong, even after I described in detail what was happening! The same call appearing on two separate bills. I simply refused to pay the bills.

Now here comes the best part. After they finally straightened out the problem, I had held back on \$114 and some change for those calls and it was appearing as \$114 Credit on my bill! After I was assured that everything was OK, the next bill came around and I was still being billed for calls from my sister's old number. By now it was Aug-Sep '87. Finally, as a software engineer, I realized how this problem could be fixed. I cancelled any affiliation I had with US Sprint (by now, several accounts, three calling cards etc. (also, the older calling cards were still active, I think)) and waited until I received that final check for \$114 and some change. At this point, I felt comfortable enough that all the software including, rates, billing, accounts payable and accounts receivable was reset. And I started a new account. By then it was

Nov-Dec '87. Haven't had any problems since! I think since then US Sprint punted the old accounting system and has been through two revs of a new one.

joe.toth

---

### **✂ You think YOU have problems with your telephone company?**

*Warren Levy <warrenl@uunet.uu.net>*

*Fri, 27 Apr 90 16:25:17 -0400*

In the fall/winter of 1983-84 my wife, Roma, and I were living in Family Student Housing on the campus of the University of California, Santa Cruz. On 3 separate occasions in a period of approx. 3 months, the telephone in our apartment (serviced by what was then known as "Pacific Telephone", now "Pacific Bell") was dead. Each time the Pac Tel serviceman came out, he checked the wires and eventually got the phone working again. A few weeks after the third event, a new person moved into our apartment complex a few apartments away. One Sunday, my father-in-law called and at almost the same time I answered and this new neighbor answered (the phone in her apartment rang). I asked her name (Marcy) and found out she lived in the same complex. I then called Pac Tel and another serviceman came out to fix the problem; he checked and changed the wiring. When the bill came, I found several calls listed that we had not made. I contacted Pac Tel Billing who backtraced the phone numbers to the actual locations. I was then asked if I knew these people or businesses called (one was a "Lyon's Restaurant" which I had never heard of at the time). Since the billing rep believed me (I related the whole story), she removed the calls from my bill (I believe it was less than 5). I may still have that bill buried deep in my files. I had no problems after that. I hope this helps.

Warren Levy, The Santa Cruz Operation, Inc., 425 Encinal Street,  
Santa Cruz, CA 95061 +1 (408) 425-7222

---

### **✂ Blaming it on the computer?**

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

*Fri, 27 Apr 90 4:09:32 EDT*

The stories of crossed lines remind me of the oldest RISK of all -- blaming things on the computer that humans do.

Almost 20 years ago, when I was younger and less responsible, a "friend" had two phone lines. He hooked up a circuit to conference them and play the whole thing through a loudspeaker with no mic on the line -- not hard to do.

Then he would go and call two parties and connect them, to listen to the fun. Much more creative than plain prank calling. When random parties got boring, he tried connecting the only two people in the book with an unusual name, hoping they would be related. Sometimes they were, but the most amusing exchange went on for several minutes between two unrelated Mr. Vandenbroeks. Several times, they would say:

"Who is calling?"

"Mr. Vandenbroek."

"Yes?"

Unaware that they had the same name. On to the RISK... In all these cases, the parties connected attributed the double call to crossed wires -- as though it happened all the time. Prior to this digest I had not heard of actual switch defects ringing two people and connecting them for no reason. And not two relatives, or employee and boss. Nobody thought to attribute it to malicious youngsters.

Today, every yuppie kid has a house with a two line phone with a conference button. No knowledge of circuits required. If my immature "friend" did it then, it must be a regular event today. Yet we jump to blaming the equipment.

Brad Templeton, ClariNet Communications Corp. -- Waterloo, Ontario 519/884-7473

---

**✉ Re: Risky McDonald's comrade...[RISKS 9:83]**

*Charles Youman (youman@mdf.mitre.org) <m14817@mwunix.mitre.org>  
Thu, 26 Apr 90 15:19:20 EDT*

David Gursky may understand queues, but I think he misunderstands their application in the USSR. To make a typical purchase you have to wait in three queues: the first to select your merchandise, the second to pay for it, and the third to pick up your purchase. By no stretch of the imagination should it be considered efficient. The only shortage of Qs in the USSR is in the Cyrillic alphabet.



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 9: Issue 88

Wednesday 2 May 1990

## Contents

- [Booby-trapped contracted software](#)  
[Tom Kopp](#)
- [Death rate inflated in St. Bruno area, health report finds](#)  
[David Sherman](#)
- [Software Bug Causes Shuttle Countdown Hold at T-31 Seconds](#)  
[Karl Lehenbauer](#)
- [Criticism of "Glass Cockpits" \(1\) and \(2\)](#)  
[Martyn Thomas](#)
- [A320 Bangalore crash](#)  
[Martyn Thomas](#)
- [A320 criticisms reported](#)  
[Martyn Thomas](#)
- [Re: computer parks hundreds of cars illegally](#)  
[Andrew E. Birner](#)
- [\(Apparently\) widespread problem with census 800 number](#)  
[Timothy M. Wright](#)
- [Re: You think YOU have problems with your telephone company?](#)  
[Chris Lewis](#)
- [Telephone switch problems](#)  
[Webber](#)
- [White paper available: "Improving the Security of Your UNIX System"](#)  
[Davy Curry](#)
- [Virus found in a game software on the market](#)  
[Yoshio Oyanagi](#)
- [Re: Computers and names with special characters](#)  
[Bandy](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✉ Booby-trapped contracted software

*Tom Kopp* <[tkopp@carroll1.cc.edu](mailto:tkopp@carroll1.cc.edu)>

1 May 90 03:07:07 GMT

A programmer from Waukesha Wisconsin (Name is in the article, I won't post it

here) is to be charged with "destroying computer data" and causing damage in excess of \$2,500. If convicted, maximum penalties will be 5 years prison, and \$10,000 in fines. The programmer wrote the code such that he could shut it off at will in the future. The client refused to pay, so he killed the software.  
[Computerworld, 23 April 1990]

---

### **✂ Death rate inflated in St. Bruno area, health report finds**

*David Sherman <dave@lsuc.on.ca>  
Tue, 1 May 90 16:22:49 EDT*

Toronto Star, May 1, 1990:

Death rates in the St. Bruno school neighbourhood are not among the highest in Toronto, as city records previously showed, and in some cases are actually lower than the city-wide average.

A study by city health officials says a "computer programming error" incorrectly inflated death rates in the area by almost 100%, causing widespread concern among residents....

Corrected figures show that 12 to 13 people per 1,000 die in the neighbourhood east of the school each year... Earlier statistics claimed 22 of every 1,000 residents in that area die each year, a rate almost three times as high as the city average....

The new report said an age factor was incorrectly fed into the computer calculations, lumping together all deaths of people over age 65....

St. Bruno was built on the site of a former steel plant. The site was also once occupied by the phototoxicology and radiation testing laboratory operated by the environment ministry.

St. Bruno has remained closed since March, when teachers and students complained of unusual health problems, including six teachers who had developed fibroid tumours and three who had uterine cancer.

Shortly after the school was closed, an incorrect report said the two census districts immediately east of the school ... had the second and third highest death rates in the city.

---

### **✂ Software Bug Causes Shuttle Countdown Hold at T-31 Seconds**

*Karl Lehenbauer <karl@sugar.hackercorp.com>  
1 May 90 19:52:42 CDT (Tue)*

According to Aviation Week (April 30, 1990, pg. 24), a software problem caused a three minute hold at T-31 during the launch countdown of the shuttle mission that orbited the Hubble Space Telescope on April 24th.

At T-48 seconds, newly written software detected that the outboard external tank liquid oxygen fill and drain valve was open when it should have been closed. The ground launch sequencer (GLS) stopped the countdown clock at T-31 seconds.

George T. (Ted) Sasseen, director of shuttle engineering, said that the software changes were made after an incident that occurred on April 2nd, where a pipe burst and sprayed water over a 4,000 volt motor control assembly, shorting it and causing the launch processing system (LPS) control room to go down, prompting concern that the LPS could lose power in the last few seconds of the countdown. Sasseen said that unless oxygen is drained within nine minutes after the flow is stopped, a phenomenon called "geysering" could rupture plumbing and destroy the tank.

"So the fix was to put a purge in that [liquid oxygen] line and to put a small gas pad in it. We did that by hand after the inboard valve was closed and before the outboard valve was closed. The GLS sent its 'close outboard' command at 48 sec."

He said that about 10 sec. after this happened, "everyone looked around and said, 'Oh boy. We were dumb.'..."

Sasseen said the processing team violated one of its own cardinal rules that says: Never make a software change unless you can run it many, many times in simulations and tests. He said, "There are oddities about software changes that you don't always get the first time through. And the basic rule we violated is that it wasn't tested enough."

He said the purge/gas pad software may be removed because it is unlikely that there would be a total launch processing system launch between T-31 sec. and T-0. "But I want to emphasize that the software safed the system as it was supposed to."

To their credit, the system engineers were able to determine what the problem was and fix it within three minutes. A more cautious approach might have been to scrub the launch until a more careful analysis and review was performed.

---

### ✂ Criticism of "Glass Cockpits" (1)

*Martyn Thomas <mct@praxis.UUCP>  
Tue, 1 May 90 12:40:06 BST*

A leaked copy of the draft report by the Air Accident Investigation Branch into the Jan 1989 737-400 crash at Kegworth, UK, criticises the ergonomics and user-friendliness of the CRT and LED display systems and engine instruments, according to Flight Int'l (May 2-8). The crash occurred after the crew shut down the wrong engine following vibration caused by a fan-blade failure.

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK.

---

### ✂ Criticism of "Glass Cockpits" (2)

*Martyn Thomas <mct@praxis.UUCP>*

*Tue, 1 May 90 12:47:44 BST*

Dr Roger Green, of the RAF Institute of Aviation Medicine, gave a lecture to the Royal Aeronautical Society in late April 1990 in which he said that operating in a digital "glass cockpit" increases the likelihood that pilots will not maintain an independent mental picture of systems status and flight profile - "always necessary for critical surveillance but also for dealing with the unexpected" according to Flight Int'l (2-8 May 90).

This may have been a factor in the Korean Airlines KAL 007 navigation errors which led to it being shot down by the USSR.

Green adds that cockpit ergonomics and instrument design are not subjected to such exhaustive testing as are airframes: "The rigour with which these things are evaluated leaves a lot to be desired".

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK.

---

### **A320 Bangalore crash**

*Martyn Thomas <mct@praxis.UUCP>*

*Tue, 1 May 90 12:59:29 BST*

The report in Flight Int'l (2-8 May 1990) on the Bangalore crash makes very interesting reading. It is too detailed to summarise, and too long to post, but the account of the number of "flight modes" which the A320 went through in the two minutes before the crash, and the side-effects of each (which seem not to have been understood properly by the pilots) makes operating an A320 appear surprisingly complex and error-prone. It is certainly very different from flying a fully manual airplane, and the secondary effects (such as selecting a target altitude leading to the engines being retarded to idle, and needing several seconds to develop full power again) need to be well understood by the pilots.

I recommend the report in Flight, and I hope that someone who understands the A320 systems is able to post an analysis of what went wrong to RISKS.

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK.

---

### **A320 criticisms reported**

*Martyn Thomas <mct@praxis.UUCP>*

*Tue, 1 May 90 13:10:04 BST*

Andrew McKechnie, in a letter in Flight Int'l (May 2-8) reports that the February issue of Log (the journal of the British Airline Pilots' Association) contains two observations on the A320 systems by an A320 pilot.

"The author, who has experience of flying the A320, claims that the display of airspeed is less than compelling and also that he has 'experienced an

occasion when the autothrottle made no attempt to hold a correct speed'."

Comment by MCT: the latter point could be a misunderstanding of the active flight mode and therefore of the speed which the fly-by-wire system deemed to be correct. In other words, if the incident reported really occurred, it could be evidence of a technical malfunction OR it could be evidence of the pilot's difficulty in understanding what speed he/she had caused the computers to select as the target speed. In either case it is relevant to RISKS.

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK.

---

### **✂ Re: (Not necessarily) computer parks hundreds of cars illegally**

ZENITH <ZENITH@l66a.ladc.bull.com>

Tue, 01 May 90 14:04 PDT

I saw the TV reports (on the local NBC affiliate, Channel 5). I'd like to add a bit to what's been said so far about the (allegedly) undeserved parking tickets:

- 1) According to the news reports, the city blames the incident on human error--on the part of the officer issuing the ticket, the operator keying in the information, or both. This time (see below), they didn't try to call it a computer error; that designation came from those reporting on the story.
- 2) Illinois license plates indicate a registration type and plate number. Taxis have Taxi plates; the plate numbers end in TX, as well (e.g. 12345 TX). Livery vehicles have livery plates, with numbers ending in LV. State and local governments have their own plate types, as do some utilities. So, the same series of digits can appear on a large number of plates; other plate information must be used to distinguish among them. If the other information does not make it into the computer, for whatever reason, the ticket will be charged to the wrong plate; if the other information is garbled, the same will happen. I've had the misfortune to examine a number of parking tickets over the years; from what I've seen, the quality of the input documents (written in ink by an officer standing by the car, possibly in high winds and freezing rain) makes errors in transcription rather likely.
- 3) This is not the first time this has happened. Last time, back in about 1985, the city switched over to a ticket tracking system that didn't allow for a distinction among plate types. When the data from the old system was transferred to the new, information was lost; all Taxi, RV, Livery, etc. tickets were charged to the passenger plates with the same number. (The firm that got the contract was not based in Illinois; they had no idea what our license plates look like. If this sounds to the reader as though the contract should not have gone to this particular company, you are not alone; the FBI and several federal courts have agreed with you, if I recall correctly.)

The details above are from memory; corrections and amplifications are most welcome. The opinions are mine; they do not necessarily correspond to those held by my employer or by any organization who might happen to forward my email.

- Andrew E. Birner, Zenith Electronics Corp -- <Zenith/A\_Birner@ladc.bull.com> -

---

### **✉ (Apparently) widespread problem with census 800 number**

<twright@ATHENA.MIT.EDU>

Tue, 1 May 90 18:17:03 -0400

The recent postings about the woman in Florida and the (possibly malicious) problems involved with her phones reminded me of problems of a decidedly non-malicious problem I had involving the Census Bureau's toll free system.

Each census form sent by the Bureau of the Census was contained in an envelope on which was printed a toll-free number to call in case of any questions (800-999-1990). I had a relatively simple question, and found that one of two things happened on the 100 or so times I tried the number: either (1) a busy signal (the usual result); or (2) a few rings, a few rings (pitched slightly higher), then a click, and finally a connection, to another person with a question! The second case happened twice: both the other party and myself were rather confused for half a minute or so.

I finally did get through to an actual Census employee, and I relayed my problems with the phone system to her. She replied that other callers had relayed similar problems. I wonder if the Bureau of the Census will fix its phone system in the next ten years.

--timothy m wright--gradual student, political science, MIT

---

### **✉ Re: You think YOU have problems with your telephone company?**

Chris Lewis <clewis%eci386@uunet.UU.NET>

Tue, 1 May 1990 16:21:09 -0400

One particular scenario which is worth considering is that of intentional sabotage by active insiders. A few years back a new large telephone switch was installed in a very high profile site to serve as a demonstration of technological achievement and to garner additional sales. The switch was plagued for many months with severe problems, most along the line of partial or complete service failure, and occasionally bizarre behaviour. Made the papers many times... Rather embarrassing to say the least.

Naturally, the service provider was concerned, and involved the switch manufacturer who spent many months (and millions of dollars) analysing the hardware and software, involving both the original R&D organization and outside consultants to try to establish a cause. All to no avail.

It wasn't until the manufacturer slipped in one of their own personnel into the

on-site maintenance crew (the provider was refusing to permit this) that the problem was resolved: one of the service provider's onsite people was intentionally shorting out signals (amongst other things reasonably difficult to pinpoint after the fact).

Sorry to be so cagey. I understand that most of this has been documented in the press, but I'm not absolutely certain of the precise details, nor wish to subject the companies involved with further embarrassment. Especially since I don't know whether or not the person was charged, what with, nor whether it was successful, nor why he was doing it in the first place.

You may wish to treat this story as totally apocryphal, that's up to you, but a scenario of active inside sabotage is certainly possible and should be investigated by your contact's phone service.

Chris Lewis, Elegant Communications Inc, {uunet!attcan,utzo}!!suc!eci386!clewis

---

### **⚡ Telephone switch problems**

*<webber@psych.toronto.edu>*

*Mon, 30 Apr 90 12:20:58 EST*

My recollection of this is fuzzy, but the recent discussion of telephone switch problems eventually reminded me of some major problems experienced in Ottawa at an early Bell Northern installation. Large numbers of telephone misfunctions developed at this showcase operation, but I believe they were eventually traced to the actions of a disgruntled former employee.

I believe he was entering the equipment room and shorting conductors together. I'm sure that some Bell Northern folk who read RISKS are better informed than I on this matter; perhaps some of them could comment?

---

### **⚡ White paper available: "Improving the Security of Your UNIX System"**

*<davy@itstd.sri.com>*

*Tue, 01 May 90 19:22:29 PDT*

A new white paper from SRI International's Information and Telecommunication Sciences and Technology Division is now available.

The paper, "Improving the Security of Your UNIX System," describes measures that you as a system administrator can take to make your UNIX system(s) more secure. Oriented primarily at SunOS 4.x, most of the information covered applies equally well to any Berkeley UNIX system with or without NFS and/or Yellow Pages (NIS). Some of the information can also be applied to System V, although this is not a primary focus of the paper.

An abbreviated Table of Contents:

#### 1. INTRODUCTION

- The Internet Worm, the Wily Hacker, other break-ins
2. IMPROVING SECURITY
    - 2.1 Account Security  
Passwords, expiration dates, guest accounts, group accounts, Yellow Pages
    - 2.2 Network Security  
Trusted hosts, secure terminals, NFS, FTP, TFTP, mail, finger, modems and terminal servers, firewalls
    - 2.3 File System Security  
Setuid shell scripts, sticky bit on directories, setgid bit on directories, umask values, encrypting files, devices
  3. MONITORING SECURITY
    - 3.1 Account Security  
lastlog, utmp, wtmp, acct
    - 3.2 Network Security  
syslog, showmount
    - 3.3 File System Security  
find, checklists, backups
    - 3.4 Know Your System  
ps, who, w, ls
  4. SOFTWARE FOR IMPROVING SECURITY
    - 4.1 Obtaining Fixes and New Versions  
Sun fixes on UUNET, Berkeley fixes, SIMTEL-20 and UUNET, vendors
    - 4.2 The npasswd Command
    - 4.3 The COPS Package
    - 4.4 Sun C2 Security Features
    - 4.5 Kerberos
  5. KEEPING ABREAST OF THE BUGS
    - 5.1 CERT
    - 5.2 DDN Management Bulletins
    - 5.3 Security-related mailing lists
  6. SUGGESTED READING
  7. CONCLUSIONS
- REFERENCES
- APPENDIX A - SECURITY CHECKLIST

In order to format the paper, the "troff" text formatter and the "-ms" macro package (available with any Sun or Berkeley UNIX system) are required. You \*do not\* need a PostScript printer, unless you want to print the cover page with the SRI logo on it.

The paper is available via anonymous FTP from the host SPAM.ITSTD.SRI.COM (128.18.4.3) as the file "pub/security-doc.tar.Z". Be sure to remember to set "image" mode on the transfer. Sorry, UUCP access is not available - if you don't have Internet access, find a friend who does.

Enjoy.

Dave Curry

SRI International  
Information and Telecommunications

Sciences and Technology Division  
333 Ravenswood Avenue  
Menlo Park, CA 94025  
(415) 859-2508

davy@itstd.sri.com [Many thanks, Davy. This is a goody. PGN]

---

### ✂ Virus found in a game software on the market

Yoshio Oyanagi <oyanagi@is.tsukuba.ac.jp>

Wed, 2 May 90 22:26:08+0900

#### VIRUS FOUND IN A JAPANESE GAME SOFTWARE ON THE MARKET

Yoshio Oyanagi  
University of Tsukuba, Japan

Newspapers reported on April 24 that a virus was found in a simulation game software "FAR SIDE MOON" (9500 yen) for Sharp personal computer X68000. It has been sold by Artdink Inc. since April 13 in Japan. The virus was detected by Computer Virus Institute (Takao Yamamoto, director) of Federation of Japanese Computer Clubs.

According to Yamamoto, this virus is programmed so that it keeps inactive until July and after that data on floppy or in the computer will automatically be erased whenever one switches on the computer.

So far 3000 sets have been sold, among which half are contaminated. It is conjectured that the computers in Artdink Inc. are invaded by the virus while developping the game software.

Today (May 2) Asahi Shinbun (one of the major daily newspaper in Japan) disclosed that it succeeded in making contact with one of the virus makers. According to the report, the maker is a high school boy of age 17, who lives in Kagawa prefecture. Forty people collaborated in making the virus and got several tens of thousand yen (several hundred dollars) for each from the client, who ordered through PC network for hackers. The virus program was completed in three months and distributed secretly since last September.

Federation of Japanese Computer Clubs told that there have been two viruses (viri?) for X68000, named "Namba I" and "Namba II". "Namba I" becomes active on July 4 this year and it deletes data on the computer or floppy disks. If the computer is contaminated with both "Namba I" and "Namba II", some X68000 do not accept any floppy after 0:00 May 2. The federation has developped a vaccine and distributing it among PC shops and users. If, however, a computer is contaminated with both viruses, it does not even accept the floppy disk of the vaccine. In this case, user should bring the computer to the maker and ask to change the parts.

(crossposted to comp.risks and comp.virus)

---

**✉ Re: Computers and names with special characters (Hoffman, [RISKS-9.85](#))**

<bandy@capmkt.com>

Tue, 1 May 90 10:24:59 PDT

>... Univac/Sperry/Unisys computers, I ought to change my name to @FIN

Or perhaps @@term ? If I remember correctly the double master space character can appear anywhere in a line...



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

**Volume 9: Issue 89**

**Monday 7 May 1990**

## Contents

- [A funny thing happened at the lottery office](#)  
[Alan Hargreaves](#)
- ['Boy, 12, allegedly taps credit files'](#)  
[Ira Greenberg](#)
- [Robert T. Morris' sentencing](#)  
[PGN](#)
- [Hazards Of Office Laser Printers](#)  
[Keith Dancey](#)
- [Re: Aircraft electronics problems PIREP](#)  
[Steve Jay](#)  
[Robert Dorsett](#)
- [Re: A320 criticisms reported](#)  
[Robert Dorsett](#)
- [Phone system problems](#)  
[Gail L Barlich](#)  
[Steve Bellovin](#)  
[Andras](#)
- [Phone Switch Resets](#)  
[Avi Belinsky](#)
- [Other ways to get "Improving the Security of Your UNIX System"](#)  
[Davy Curry](#)
- [So many weapons, so little radio spectrum](#)  
[Chuq Von Rospach](#)
- [Und der Hyphisch](#)  
[Andy Behrens](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✂ A funny thing happened at the lottery office

*Alan Hargreaves* <[alan@nucs.cs.nu.oz.au](mailto:alan@nucs.cs.nu.oz.au)>  
3 May 90 10:30:06 GMT

I am not sure of the truth behind this article, but the possibilities scare me a little. It is quoted from the Sydney Daily Telegraph, 3 May 1990.

When a man visited the Minnesota lottery office with a winning ticket worth \$1000, employees looked through his records and found he owed the state that amount - and more. So he was handed a cheque for \$0.00 - and a tax form.

Alan Hargreaves, University of Newcastle, NSW 2308, Australia.

---

### ✦ **'Boy, 12, allegedly taps credit files'**

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

Wed, 2 May 1990 16:14:30 PDT

A 12-year old boy in Grosse Ile, Michigan, got into TRW's credit info system, and BBoarded various credit card numbers -- which were subsequently widely used. His mother was stunned by his arrest, and ``said he spent four to five hours each week night and up to 14 hours a day on weekends at his computer. She said she was pleased her son stayed at home." [Source: Knight-Ridder News Service item in San Jose Mercury News, around 25Apr90, clipping from Ira Greenberg, undated]

If past experience is any indication, he probably found the TRW access information on a BBoard in the first place.

---

### ✦ **Robert T. Morris' sentencing and its implications**

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

Sun, 6 May 1990 17:21:13 PDT

In case you were away from the media over the weekend, Federal District Judge Howard G. Munson pronounced sentence last Friday, 4 May, on Robert T. Morris, fining him \$10,000, requiring 400 hours of community service, and placing him on three-years' probation, plus some additional administrative expenses. (Legal costs were undoubtedly much greater than the fine, so the cost to Robert is not insignificant.)

In the final analysis, the judge made a technically elaborate ruling that the new Federal sentencing guidelines (which recommend a min-max jail-term range based on a detailed point system) were NOT APPLICABLE in this case, in part because the case did not really involve computer FRAUD, and in part because there were no COMPARABLE cases on which to base the sentencing, as required under the guidelines when there is any question as to their relevance. In so doing, the judge said he disagreed with both sides -- the prosecution, which wanted to add more points primarily because of even greater consequential (indirect) losses than had been explicitly identified during the trial, and the defense, which sought to reduce the numbers on a variety of component points. INTENT, which had been ruled largely irrelevant to the verdict, may actually have been somewhat relevant in the sentencing. [This is my own private analysis, and may not be precise enough in the legalese department.]

I conclude that this case was actually not an appropriate test of either the computer security laws or of the sentencing guidelines. On the other hand, I

think that the Government will not be discouraged by the absence of a jail term in this case, and can be expected to prosecute quite vigorously all acts of more flagrant computer misuse (e.g., sabotage, intentional denials of service, or theft of data or proprietary programs). Although RTM's "experiment" was certainly ill-conceived and flawed in its execution, his sentence is not likely to encourage others to conduct similar experiments.

I commend to you the report by Davy Curry (see his messages in [RISKS-9.88](#) and again in this issue) on how to improve the security of your Unix systems (with some implications for other computer systems as well). It is high time people with vulnerable systems did something more serious about protecting them, and his report is a useful contribution, going well beyond the Internet Worm articles of Eichin and Rochlis, Seeley, and Spafford in that it transcends the particular flaws exercised by the Worm. Remember, it may be YOUR privacy rights that are being protected, which should make the increased security a little more tolerable. On the other hand, let me once again reinforce my hopes that we can live in a less antagonistic, more open, and more ethical society in which computer security is somewhat less critical!

PGN

P.S., PRIMARILY FOR RECIPIENTS OF MULTIPLE RISKS COPIES: Speaking of SENDMAIL problems, for no apparent reason the last three previous RISKS issues have gone out with NO DUPLICATE ISSUES attributable to our originating sendmail. A few recipient sites seem to have cleaned up their acts, almost all .arpa addresses are gone, and a bunch of other problematic addresses have been relegated to a potentially higher-risk sublist. Because of the annual IEEE Oakland security bash and other activities, RISKS issues will be sporadic at best this week, and are likely to emerge at higher risk than the recent carefully-monitored issues -- when you, me, and my wizards were able to watch the mailer in progress. Perhaps on this issue the unwatched pot will boil over, but I am optimistic for a change. (The fascinating part was that the problem was hitting different addresses in different sublists each time.) [FOR THIS ISSUE ONLY, if you get multiples, a few of you should send a message to [root@csl.sri.com](mailto:root@csl.sri.com), although the problem would not get taken care of until later today -- because it is too early for wizards (only mad dogs and RISKS moderators). On the other hand, running sendmail in the wee hours seems to minimize the problem, because the originating host and the network are livelier! In any case, thanks for your patience.] By the way, I hope that there are no lawsuits against RISKS for causing denials of service in overflowing your mailbox. On the other hand, I am surprised I haven't heard more complaints about my boring you with too many messages about sendmail problems and telephone glitches (which seem to be dying down). But the risks are there... PGN

---

### **✂ Hazards Of Office Laser Printers**

*<kgd@informatics.rutherford.ac.uk>*

*Fri, 4 May 90 13:14:02 BST*

Some fifteen months ago, in [RISKS-8.21](#), I placed a request for information on the possible health hazards of office Laser Printers.

I received a small flurry of replies, a significant proportion of which were simply expressing similar concern. Facts and figures were very thin on the ground.

At the same time I attempted a literature search which illustrated just how few studies on the subject had been made.

I wrote to Hewlett Packard seeking advice, but received no reply.

My own employers' Health & Safety personnel found "no risk".

The data I had received did not amount to much, but a report in The Guardian newspaper (UK), published on April 26th 1990, has added further information that warrants some interest...

>From my own efforts, I understood the possible hazards to be:

(a) mutagenic and/or carcinogenic compounds contained (and thereby released into the atmosphere) in the toner;

(b) poisonous compounds on the drum; and

(c) toxic gasses generated by the high electrical discharges involved.

(A) Jeffrey Mogul wrote that Digital supply printers, with Ricoh marking engines, the replacement toner cartridge kits of which contain "Material Safety Data Sheets". These list under "hazardous ingredients" Ferrosiferrous oxide, Styrene Acrylic resin, "dye" and carbon black.

The toxicity of the oxide is described as zero. That of the resin as being rendered biologically inert by the polymerisation process. The "dye" is not discussed. Carbon black has been subject to toxicity and carcinogenic exposure experiments. One view is that while carbon black particulates contain some molecules of carcinogenic materials, the carcinogens are apparently held tightly and are not eluted by water, gastric juices or blood plasma.

LOFROTH, HEFNER, ALFHEIM and MOLLER, 1980, "Mutagenic activity in photocopies", Science, 209, 1037-1039. Using a bacterial assay technique, extracts from several different photocopies were shown to be mutagenic. The evidence, they suggest, is that compounds in the toners used are responsible for this mutagenic activity.

SONNINO and PAVAN, 1984, "Possible hazards from laser printers". In Ergonomics and Health in Modern Offices, (GRANDJEAN (Ed)), Section A: The ambient environment in offices (Taylor & Francis, London), 82-85. Tested five laser printers for optical, radiation and chemical hazards. No evidence of any appreciable risk to operators was found.

Me: ERGONOMICS has ventured to regard the toner and cleaning agents "of possible greater concern" than the production of gasses. But we shall see.

(B) Not much on the drum compounds. CLARIDGE, 1983 "Photocopiers: an

office hazard". Environmental Health, 91(9), 246-247. Describes the possible hazards associated with the use of photocopiers, and presents recommendations. Among subjects considered is the photoconductor (selenium).

(C) Several people, including Brad Yearwood, pointed to the dangers inherent in the production of ozone and oxygen radicals. Brad mentioned that the Canon LBP-8 engine uses a copper wool catalytic filter.

AKTIONSGRUPPEN ARBEJDERE AKADEMIKERE, 1981 "Photocopiers and health hazards" c/o B Christensen, Arnesvej 44, 2700 Bronshoj, Denmark. Besides warning of the possible health hazards of chemicals used in toners (carbon black with aromatic polycyclic hydrocarbons and nitropyrenes, thermoplastic resins) and the evidence for mutagenic and carcinogenic effects of these toners, also covers the effects of ozone, selenium and organic solvents on health.

>From "The Guardian", April 26th, 1990:

A Science correspondent, Barry Fox, reported seeing a strange device underneath a Laser Printer in a University in Denmark. "Oh, that's an ozone filter" was the explanation, "most laser printers in Denmark have them".

Fox reported never having heard the suggestion that such a device was required...

"Ozone is an unstable form of oxygen, O<sub>3</sub>, produced by high voltages and electrical discharges... So they (laser printers) generate ozone. Despite the tangy smell, best described as the smell of electricity, ozone is not good for health: just the opposite, in fact.

...Ozone soon breaks down into oxygen, but does so while attacking just about anything except glass and some stainless steels.

...The Health and Safety Executive (UK body) recommends an exposure limit of 0.1 parts ozone per million of air, averaged over an eight hour day, with no 15 minute peak greater than 0.3ppm. Even at 0.1ppm, premature ageing may eventually result, and in the short term, 0.1ppm can cause eye, nose and throat irritation. At 0.5ppm nausea and headaches may occur.

Exposure for two hours at 1.5ppm typically results in coughs and excessive sputum. At 50ppm, a 30 minute exposure may be fatal.

'Areas must be equipped with adequate ventilation and extraction facilities' warns the HSE...

...Office equipment is usually fitted with filters, containing activated carbon to break down ozone. When factory fresh, these filters reduce ozone to well below the HSE levels. But filters are small and lose efficiency with time, especially if clogged with dust (paper, toner etc), so clogging is faster if ventilation is poor. And ozone is more dangerous when ventilation is poor. Ozone can often be smelled while printing, especially near the outlet

of the machine's internal fan.

...When I (Barry Fox) started asking questions I was appalled at the lack of interest among firms selling office equipment {mentions Hewlett-Packard - see my experience of same, above, Apple and IBM}...

...Then I (Barry Fox) tracked down the firm which makes add-on filters... Dansk Teknologi of Copenhagen started making its Minozon unit in the summer of 1988 and sold 8000 in the first year. (It) is a flat plate... containing a large bed of activated carbon through which air from the printer discharges... (It) is around 50 times larger than (the inbuilt filters).

The Department of Environment Technology, at the Danish Institute of Technology, tested the Minozon filter and found that it remained fully effective even after continuously printing 10,000 A4 pages... (They) cost 300 to 400 pounds sterling in the UK.

At first sight it would seem cheaper and simpler ... to change the filters built into (the) printers. But, absurdly, built-in printer filters are often not designed for do-it-yourself replacement.

After writing about the ozone problem in New Scientist I (Barry Fox) received many enquiries... IBM thought I had been 'wound up' by the firm selling the add-on filters used in Denmark. Apple remained dormant. HP, however, confirmed it had 'escalated the whole issue of ozone filters' and made 'strong recommendations' that filter changing guidelines be incorporated in user manuals.

...The short term advice is: if you smell ozone while printing, open the windows."

Me: depends which way the wind is blowing :-). Since it is not possible to tell when the in-built catalytic filter is exhausted, and identification of ozone's characteristic smell is uncertain, \*active\* ventilation should be a requirement before installation of laser printers is considered within habitually occupied offices.

Any further comments, anyone?

Keith Dancey, Rutherford Appleton Laboratory, UK.

---

**✂ Re: Aircraft electronics problems PIREP (188 knots?) ([RISKS-9.85](#))**

Steve Jay <!shj@ultra.UUCP>  
Sat, 28 Apr 90 00:51:11 GMT

>At 3,000 feet inbound on the Instrument Landing System localiser we were  
>experiencing westerly winds of 188 knots

This just doesn't seem believable to me. This is higher wind velocity than in the strongest hurricanes. Does anyone have any confirming information that

there really were winds like that?

Steve Jay, Ultra Network Technologies / 101 Dagget Drive / San Jose, CA 95134

---

**✂ Re: Aircraft electronics problems PIREP (188 knots?)**

*Robert Dorsett <rd@walt.cc.utexas.edu>*

*Wed, 2 May 1990 19:26:58 CDT*

When I read it, I assumed that it was another indication of a glitch in the FMCS software. Listening to Austin ATC, I've noticed a tendency for pilots in glass cockpits to depend very heavily on the FMCS when giving such information. When the FMCS is down, they often reply "unable" to give the requested information. In real life, all they have to do to get to their destination is track a VOR station inbound; that provides an automatic wind correction. Then it's just a case of guesstimating groundspeed and cross-checking that with the (computerized) flight plan, to judge the arrival time. So there's not much incentive to keep basic nav skills, like determining the wind vector, alive.

Now, as for whether it's POSSIBLE... not likely, unless they were in a major storm. And if they were, why weren't upper-level wind speeds very high? And why would they have continued the approach? At high altitudes, winds can get up to that speed, with no major problems for aircraft flying through them, (except in boundary regions), but near the surface, 188-knot winds would likely result in monstrous wind shear (as a result of the mechanical interaction of winds with the surface). At 80 knots, there would be pretty bad wind shear. And even 80 knots is beyond the crosswind capability of jet transport category aircraft.

Nah, it was a glitch. Adds more drama to the primary story of the avionics going haywire on the go-around, though. I would LIKE to think that the crew was mentioning this as an event in a continuing sequence of failure, and didn't actually believe it had 188 knot winds... :-)

---

**✂ Re: A320 criticisms reported**

*Robert Dorsett <rd@walt.cc.utexas.edu>*

*Wed, 2 May 90 19:53:06 -0500*

>The author, who has experience of flying the A320, claims that the display  
>of airspeed is less than compelling

It's noteworthy that the A320's airspeed display is a "tape" instrument, with white letters set on a gray "tape," all mounted on a black background. Current airspeed is indicated by a single red "lubber line"; the speed tape scrolls behind that line. This is in contrast to the tape airspeed displays on the 747-400 and MD-11, which have a "window" in which the current airspeed is displayed, in a much larger font. The latter approach is more in keeping with the results of real-life experience with analog tape (such as is used on the C-141 and C-5A) and drum digital counters. I don't know what Airbus was

thinking when it decided on a red lubber line: it's an intuitively bad design, and has earned criticism from many pilots.

It's probable that the use of tape displays, as a category of indicators, is predicated entirely on the economics and desirability of having CRT flight displays. Screen real estate is at a premium. There is no demonstrable UI advantage to using tape instruments; in fact, at least some research suggests the contrary. Tape instruments are prone to misreadings.

Robert Dorsett, Moderator, Aeronautics Mailing List

---

## **✂ Phone system problems**

*Gail L Barlich <glb%beta@LANL.GOV>*

*Wed, 2 May 90 12:17:44 MDT*

I began my undergraduate education at a church-related college in Texas. To handle long distance calls from dorm phones the phone company issued everyone "student billing cards." The phone company waved the deposit because of the reputation (?) of the school.

Then I transferred and again decided to live in the dorm. I contacted the phone company and explained how I had a "student" card in Texas. They had a similar deal but required that a hefty deposit remain on account. I explained that I had a card in Texas with no deposit. The woman suggested that I write a letter about my previous account and include my card number if possible. A few weeks later I was issued a "student" card without a deposit because the "the computer" showed that my Texas card was actually a "normal" billing card and I had a good payment history. They could not issue a "normal" card for a dorm resident.

Each new school year I would call the phone company and confirm that my card was still active. Each year I had the same card number.

Well, my last year I got lazy. I just began using it like usual and never got a complaint from an operator. I was making calls during the day related to job hunting, so I expected horrible bills. The months went by, but no bills came. I called the phone company in December. Somehow I had visions of the university holding my diploma if I had outstanding bills. The phone person insisted that my account showed zero. Then I talked to the supervisor, and he also stated that my account was entirely paid with no phone calls on record for my card or my dorm phone number. I told him exactly where I had been calling and the charges I expected. One week later a programmer called and congratulated me on beating the phone system. Apparently my "student" card had some kind of odd designator on the number that merged it into the "normal" card database. The phone company had actually terminated the "student" card program many months before. My number had survived but with no connections into billing. The employee informed me that my card had been terminated in good standing.

So I got out into the real world and called to get a telephone hooked up. I carefully gave them both "student" numbers. They told me that no deposit

would be required because of my excellent payment history...

---

## ✂ Phone system problems

<smb@ulysses.att.com>

Wed, 02 May 90 14:40:19 EDT

I don't know if these two stories shed any light on the problems, but they're illustrative of system-level failures.

When I lived in Durham, NC, during the early 1970s, the local phone system (GTE) did not have Automatic Number Identification (ANI) on long-distance calls. As a result, whenever you placed such a call (and you could direct-dial), an operator would come online and ask what number you were calling from. The possibilities for error and fraud are, of course, obvious, and it was always a subject of much discussion what checking was done. Did they at least have information on your exchange? Could they tell if the alleged calling line was actually busy? And most important, what happened to misattributed calls? One prevalent local rumor had it that such calls, when challenged, were randomly assigned to other phone lines, in proportion to the number of actual calls. That theory always seemed improbable, but...

One day, we receive a bill showing a call to %Fayetteville. Now, we knew that none of us had ever called Fayetteville, much less %Fayetteville, so we went through the usual ritual of calling up to complain. The response this time was totally unexpected. ``I'm sorry, sir, but our records show that that charge has already been investigated from a previous bill, and found to be justified." That was totally erroneous, and we could prove it -- we had all of our phone bills going back for quite some time. I told the agent this; she relented, and took the charge off the bill.

We never did figure out where that call came from, what the % meant, or why GTE tried to claim that it was a call we had previously challenged.

The second incident happened several years later, in Chapel Hill, after Southern Bell had (by order of the State Utilities Commission) bought out the local university-owned phone system, but before they'd had a chance to upgrade it to use a switch not seemingly hand-built by Strowger himself. They were running out of phone numbers on the exchanges, and they didn't want to expand the old switch because they were frantically trying to replace it with an ESS. So new customers, especially in the southern part of the service, were assigned phone numbers on the university Centrex system, and hence could abbreviate much of their dialing. In particular, when I wanted to call the port selector at the Comp Center, I'd dial 3-9911, instead of 933-9911. Now, I had one of the old mechanical, card-operated autodialers that somehow the local phone company didn't know about. This beast dialed quickly (for a pulse dialer), and sometimes the

switch couldn't keep up. So, when the second digit arrived too soon, it would reset, and give me dial tone again -- just in time for the last three digits, 911...

The rest of the Chapel Hill phone system was on a par with the switch, but I'll omit the details; they belong in Telecom Digest, or maybe the Museum of Horrors.

--Steve Bellovin

---

### **✉ more Phone Problems**

*<andras@sbc.suny.edu>*

*Wed, 2 May 90 15:40:08 EDT*

This is in relation to phone company billing practices, both ATT and Sprint. First an observation about AT&T and "instant credit".

When one gets a bad international line, AT&T does not expect payment for the call. One can just call the operator, tell them what happened, and forget about it. Well, this is incorrect: one must call twice. The first call is right after the problem occurs. The operators cheerfully agree to immediate credit. At the end of the month, lo and behold, the call is still billed. This gives rise to a second call which finally settles the matter.

It happened to me, and others I asked (I'm a graduate student, with lots of foreign nationals in the department.) I've once seen a friend's bill with a dozen or so failed overseas calls. All one minute long, all one right after another. All called in to the operator as soon as they were made.

It's enough to make one suspect that it's deliberate; corporate customers especially might not keep accurate track of all short overseas calls.

Now the Sprint story.

A few months ago (Jan 20), I had occasion to make an international call to Europe (Romania). Not being up-to-date on the latest prices (I asked the operators, and apparently prices are no longer distributed; I guess you're expected to call every time you want to check.) I called the long-distance carriers I knew about, found that Sprint had the lowest rates by a fair margin, so I called them through their access number (my primary carrier is AT&T).

When the bill arrived, it was about 50% higher than I expected. I called Sprint (Mar 2), and asked about their rates again, and they again quoted the same numbers. I then mentioned the bill. The operator did some more checking, then announced that yes, apparently they changed their rates at the beginning of the year (Jan 1), and that billing was done based on the new rates. She was apologetic, and said she would call this to the company's attention.

Apparently Sprint was still giving out the old rates, three months after new

rates were in effect!

Andras

---

**☛ Phone Switch Resets (Webber, [RISKS-9.88](#))**

*Avi Belinsky <abelinsk@sunee.waterloo.edu>*

*Thu, 3 May 90 01:14:28 EDT*

Some interesting but unimportant trivia about this case. When I used to work at Bell Northern Research (research arm of Northern Telecom) someone in the know told me about this story. Apparently it was known internally as the gold ring problem. A disgruntled employee would run his gold wedding ring along the back of the Printed Circuit Boards and short the system, resetting it.

For a telephone switch provider, where down time called for in tenders is one hour per 40 years, the damage to their reputation was enormous. Apparently they lost millions tracking down this "bug" and even more in lost sales from the bad reputation this flagship switch generated. I believe they tracked it down by matching operator logs with system resets.

I heard that the operator was later found floating dead in the Ottawa river :-)

Avi Belinsky            Electrical Engineering, University of Waterloo

---

**☛ Other ways to get "Improving the Security of Your UNIX System"**

*<davy@itstd.sri.com>*

*Thu, 03 May 90 16:12:21 PDT*

Due to the overwhelming demand (1000 FTP connections in 24 hours) for my paper, "Improving the Security of Your UNIX System," I have made it available via some other sources, listed below.

Thanks to the system administrators at these sites who've allowed me to distribute the paper through their machines.

Dave Curry, SRI International

Last update: May 3, 1990

The SRI International white paper, "Improving the Security of Your UNIX System," may be obtained via the following methods:

**1. ANONYMOUS FTP**

The document is available via anonymous FTP from the following hosts:

(West Coast) Host: SPAM.ITSTD.SRI.COM

Addr: 128.18.4.3

File: pub/security-doc.tar.Z

(West Coast) Host: GATEKEEPER.DEC.COM

Addr: 16.1.0.2  
File: pub/doc/sri-security-doc.tar.Z  
(East Coast) Host: UUNET.UU.NET  
Addr: 192.48.96.2  
File: doc/security-doc.tar.Z  
(Midwest) Host: TUT.CIS.OHIO-STATE.EDU  
Addr: 128.146.8.60  
File: pub/security/security-doc.tar.Z  
(MILNET) Host: WSMR-SIMTEL20.ARMY.MIL  
Addr: 26.2.0.74  
File: pd2:<unix-c.info>security-doc.tar-z

Transfer the file in "binary" mode from SPAM, TUT and UUNET, or "tenex" mode from SIMTEL-20. After you get the file, execute the commands:

```
% uncompress security-doc.tar.Z  
% tar xf security-doc  
% cd security-doc
```

And now consult the README file.

## 2. UUCP

UUNET subscribers can obtain the document via UUCP from UUNET using a command of the form

```
uucp uUNET!~/doc/security-doc.tar.Z destination-filename
```

UUCP sites that are not UUNET subscribers will not be able to get it directly through them, but may be able to find another UUCP neighbor who has the file.

You can obtain the file via "anonymous" UUCP from Ohio State University by placing the following line in your L.sys file:

```
#  
# Direct Trailblazer  
#  
osu-cis Any ACU 19200 1-614-292-5112 in:--in:--in: Uanon  
#  
# Micom port selector, at 1200, 2400, or 9600 bps.  
# Replace ##'s below with 12, 24, or 96 (both speed and phone number).  
#  
osu-cis Any ACU ##00 1-614-292-31## "" \r\c Name? osu-cis nected \c GO \d\r\d\r\d\r in:--in:--in: Uanon
```

and then issue the command

```
uucp osu-cis!~/security/security-doc.tar.Z destination-filename
```

## 3. BITNET

BITNET users may obtain the document via the European TRICKLE servers from the UNIX-SW archives. To do this, use the TELL command as follows:

```
TELL TRICKLE AT SOMEHOST /PDGET <UNIX-SW.INFO>SECURITY-DOC.TAR-Z
```

where SOMEHOST is one of:

DKTC11 Denmark  
TREARN Turkey  
IMIPOLI Italy  
BANUFS11 Belgium  
AWIWUW11 Austria  
DBOFUB11 Germany  
EB0UB011 Spain

There are no TRICKLE hosts in the U.S.; the Europeans are graciously allowing U.S. BITNET users to access their machines. Please be kind to them. Sorry, but the LISTSERV machines at RPIECS and NDSUVM do not provide access to the UNIX-SW repository.

The file will arrive in BITSEND, NETDATA format. You should use the BITRCV command from RDRLIST to get the file. (I have no idea what this means -- go find an IBM guru if you don't know either.)

This will be a BINARY file. You won't be able to do much of anything with it on an IBM system. Instead, transfer it to a UNIX system, and then uncompress it and extract the tar file, and then format things. See above under "FTP" for how to do this.

#### 4. ELECTRONIC MAIL

The document may also be obtained from the SUN-SPOTS archive server located on host TITAN.RICE.EDU. In order to request the document, send a note with the word

help

to "archive-server@titan.rice.edu" (uunet!rice!archive-server).

I don't, as of this writing, know what the path to the document will be, so you'll have to use the "index" command to hunt around for it. It will probably live in the "sun-source" directory, so you may want to just send "index sun-source" instead of "help".

#### 5. DECNET

DECNET users can obtain the file by copying

```
DECWRL::"/pub/doc/sri-security-doc.tar.Z"
```

by using the COPY command, or whatever.

---

### So many weapons, so little radio spectrum

*The Bounty Hunter* <chuq@Apple.COM>  
5 May 90 02:34:32 GMT

>From the May, 1990 issue of Monitoring Times, Page 4:

## Electronic Blizzard Brings Down U.S. Planes

The Scene is Libya, 1986. High in the sky, an armada of 33 high-tech U.S. fighter planes begin their attack. But something is wrong. One plane, carrying two crew members, crashes. Of the surviving 32 planes -- including five F-11's -- seven are unable to get off even a single shot. The probably reason: an electronic blizzard that, according to Pentagon officials, came not from the Libyans but from high-powered U.S. military transmitters that filled the night sky with electronic signals designed to jam Libya's anti-aircraft defenses, hunt down targets, guide weapons and communicate.

According to Air Force Colonel Charles Quisenberry, during the Libran strike, U.S. weapons "were interfering with each other." Numerous U.S. weapons, some of which were electronically guided, went astray during the attack, damaging three foreign embassies and diplomatic residences, uncluding those of France and Japan.

Further, says Quisenberry, some of this interference can "actually effect the ... aircraft's flight controls as well as its fuel controls," either putting a plan into an uncontrolled turn or dive or turning off its fuel supply.

The Pentagon recently finished a classified seven-month investigation of the prolem which led officials to order a more detailed three-year probe. Preliminary studies of one war plan shows "thousands of [frequency] conflics" among weapons. Says Quisenberry, "There are major, major problems out there..."

---

### ✈ Und der Hyphisch ([RISKS-9.83](#))

Andy Behrens <andyb@coat.com>

Thu, 3 May 90 15:13:13 EDT

If the Social Security office stores their database on a PC, and wants to hack the program so it would allow hypkens, I'm sure they could find a PC Hacker to do the job. On the other hand, if they use a Mac and need someone to mess with the program, wouldn't they have to hire a Mac Messer?

[Ah, Mac(k) the Knife. A few of you remarked on my earlier reference to "Und der Haifisch" (the opening words of the Three-Penny Opera, And the shark has pretty teeth, auf deutsch). Thanks, Andy! 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 9: Issue 90

Thursday 10 May 1990

## Contents

- [The Mayor and the EMail](#)  
[John Markoff](#)
- [Democratic bug in AppleLink!](#)  
[Hector Rojas](#)
- [`Hacker' alters phone services](#)  
[David G. Novick](#)
- [Re: A funny thing happened at the lottery office](#)  
[Mike Beede](#)  
[Emmett Hogan](#)
- [Risk of Unauthorized Access to TRW Credit Database](#)  
[Larry Lippman](#)
- [Unusual traffic light behaviour](#)  
[Andy Coombes](#)
- [High School Boy's Story was a Fake](#)  
[Yoshio Oyanagi](#)
- [More about Sharp's Viri in Japan](#)  
[Yoshio Oyanagi](#)
- [ARMY wants computer viruses for battlefield use](#)  
[Gary McClelland](#)
- [A-320 avionics malfunctions](#)  
[Vic Riley](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **The Mayor and the EMail**

*John Markoff* <[markoff@nisc.nyser.net](mailto:markoff@nisc.nyser.net)>

*Mon, 7 May 90 18:34:43 -0500*

From The New York Times, May 4, 1990, Friday, Late Edition - Final  
Section A; Page 12, Column 3.

In Colorado, a Furor Over Computer Mail (By JOHN MARKOFF)

For more than a year, the Mayor of Colorado Springs read the electronic

messages about city business that members of the City Council sent to one another from computers at their homes. The disclosure of the Mayor's mail perusal has not only touched off a bitter political dispute in the city but has also put a spotlight on problems in reconciling advances in computer technology with laws on open meetings, public records and personal privacy.

The Mayor, Robert Isaac, has defended his actions, saying he monitored the council members' messages because he was concerned that they were using the system to hold illegal caucuses. Under Colorado law, City Council business, with a few exceptions, must be conducted at public forums.

'Public vs. Private Conflict'

"It's a good example of public versus private conflict in the face of new technology," said Carol Gould, a professor at the Stevens Institute of Technology, who has studied the ethical implications of computer networks. "It's a problem that computer technology exacerbates, and it points to the importance of designing systems that distinguish between private communications and open public discussions."

More broadly, the case has raised concern that actions like those of Mayor Isaac could undermine public trust in computerized technology designed to promote efficiency in civic affairs and to allow more residents to participate in their local government.

"It's serious," said Marc Rotenberg, national director of the Computer Professionals for Social Responsibility, an advocacy group. "Because users of electronic mail systems should have a fundamental expectation of confidentiality, when that expectation is breached, the value of the network is undermined and a chilling effect on future use is likely to result."

Some City Council members said that even if the Mayor's actions were legal, they undermined the political system. "I did not know the Mayor was reviewing our mail," said Mary Lou Makepeace, a Council member. "At the very least, it's bad manners." But at least two of the nine members said they had been aware that the Mayor had access to computer printouts of messages stored in the system. Only six members of the Council were using the computer system. \$22,000 Computer System At the heart of the dispute is a computer system the Council purchased in November 1988. The \$22,000 system included portable computers for Council members to permit them to send and receive electronic messages while they were away from the city offices. The base computer in the city offices also enabled officials to post public notices that city residents could see by calling the system.

The Mayor's ability to monitor the messages was curtailed in February after several members of the Council became curious about his knowledge of issues that had been discussed on the computer. After they raised the issue, City Manager Roy Pederson decided the messages were as private as telephone calls and should therefore be read only by those to whom they were addressed. He ordered that a city secretary stop making copies of the messages from the base computer at the city offices.

The Mayor confirmed that he had been reading the messages by complaining to the Council later that his access to them had been cut off. Mayor Isaac, who will

become president of the United States Conference of Mayors in June, said he thought the Council members understood that all the messages sent on the computers could be read by anyone with access to the system.

#### He Seeks Public Access

Mayor Isaac told the Council that he had received copies so he would know what everyone on the Council was talking about. He said he believed that each Council member should see copies of the materials and that they should be open to the news media as well to make sure the Council was complying with the state law on conducting business in public. The Mayor also said he believed that the information on the computer, including the Council members' messages, should be accessible to the public.

"It's still an issue at this point," said Wayne Fisher, a Council member who says he is considering filing a complaint with the Federal Bureau of Investigation under the 1986 Federal Electronic Communications Privacy Act. "Several times on the system I sent messages to other Council members that said, 'Boy, am I glad the Mayor can't read this.' "

The law requires operators of public electronic communications systems to protect the privacy of messages on their system. The law distinguishes between public systems and those that are for private use. But the law also places some restrictions on privately maintained systems. Violations carry a maximum penalty of five years in prison.

Until recently Mr. Isaac, a three-term Republican, was considering running as a Republican candidate for governor, but he decided not to enter the primary. He said his decision to withdraw was not related to the electronic mail controversy.

#### Mayor Opposed the System

But Mayor Isaac said he believed the issue was being used for attacks by Democratic politicians. "I personally don't think we ought to be paying tax money for private telecommunications," said Mr. Isaac, who had opposed purchasing the computer system.

The City Attorney, James Colvin, who is now reviewing the city's policy regarding the use of the electronic mail system, said he did not believe that the Mayor's actions had violated the communications privacy law. But legal experts said it was possible the law had been violated.

"I think that he could be in some trouble," said John Podesta, a consultant in the District of Columbia, who formerly served as legal counsel to Senator Patrick J. Leahy, Democrat of Vermont, the principal sponsor of the communications law. Mr. Podesta said he was concerned that the Colorado Springs controversy would cause other cities to think twice about relying on similar computer systems. "People are going to worry that if they plug into these systems it will be like bringing Big Brother into their households," he said.

---

## **⚡ Democratic bug in AppleLink!**

*Axis, Hector Rojas, Chile,ICC <LAICHI.SPT@AppleLink.Apple.COM>  
08 May 90 19:17 GMT*

There is a peculiar bug in the AppleLink application which, taking into account the country in which I currently live (Chile) made me sit up and grin. (The AppleLink application is a nice front end for Apple Computer's worldwide electronic mail and bulletin board system.)

This is the bug:

- 1 Write a new memo and save it using the name "General".
- 2 Quit to the Finder or switch to it if you're using MultiFinder.
- 3 Now try to find the file "General". It's not there!

This problem occurs in both AppleLink version 4 and version 5. I don't have a copy of version 5.1, so I can't tell if it happens there as well. The problem is repeatable 100%. A document that is supposedly saved as "General" will cause some disk activity as if it is being saved, but you will never find anything on your disk. As far as I only it only happens with documents saved as "General".

You can imagine how baffled I was the first time it happened to me, just after finishing a lengthy letter. I looked all over the place using disk utilities, searching utilities, etc. (no, you hackers out there: the file is not "invisible" either). It was gone.

However, after a while the logic behind the "General's disappearing act" dawned on me: some of you may remember that only two months ago, Chile's former dictatorial regime, headed by General Augusto Pinochet, was replaced by the democratically elected president Patricio Aylwin.

So remember from now on: General will always disappear :)

-- Thomas Fruin    Apple Chile

AppleLink: LAICHI.SPT (laichi.spt@applelink.apple.com)  
Internet: tafruin@heraldo.apple.cl

---

## **⚡ `Hacker' alters phone services**

*"David G. Novick" <novick@cse.ogi.edu>  
Tue, 8 May 90 09:46:06 -0700*

The Spring, 1990, issue of Visions, the Oregon Graduate Institute's quarterly magazine, has an interesting article on a man who broke into telephone computers, creating the kinds of disruptions that have been discussed lately on RISKS. The programmer, named Corey Lindsly, lives in Portland, OR. He was eventually arrested and pled guilty to a felony count of stealing long-distance phone service. Here is an excerpt.

--David

Confessions of a Computer Hacker  
by Michael Rose  
Visions (Oregon Graduate Institute quarterly magazine)  
Spring, 1990

...

Perhaps the most disturbing part of Lindsly's adventures was his penetration of AT&T Switching Control Center Systems. These sensitive computers support long distance telephone service. System administrators for 17 of these computers spent over 520 hours mopping up Lindsly's damages.

According to [AT&T New Jersey manager of corporate security Allen] Thompson, Lindsly could have "severely disrupted" the nation's telephone service.

Lindsly, however, bristles at the suggestion of his doing potentially dangerous stunts. Anything beyond harmless pranks is "beneath the hacker ethic and uncouth," he says.

He does admit to disconnecting phones, changing billing status, and adding custom calling features. He also likes to convert residential lines to coin class service, so when the unwitting homeowner picked up his phone, a recorded voice would tell him to deposit 25 cents.

"Swapping people's phone numbers ... now that was great trick," he recalls, with obvious amusement. "You would have your next door neighbor's number and he would have yours, and people would call you and and ask for your neighbor, and vice versa, and everyone's getting totally confused."

---

### **✂ Re: A funny thing happened at the lottery office (RISK-9.89)**

*Mike Beede <beede@SCTC.COM>  
Mon, 7 May 90 09:20:17 CDT*

>When a man visited the Minnesota lottery office with a winning ticket worth >\$1000, employees looked through his records and found he owed the state that >amount - and more. So he was handed a cheque for \$0.00 - and a tax form.

Completely true, and has happened a number of times already. The amounts mentioned in local papers range up to the maximum \$5,000 prize.

Quite a lot of controversy about introducing a state lottery here -- a columnist made an interesting observation: this is the first time the state of Minnesota (known as a very high-tax state) has ever offered a tax break based on intelligence. I guess I agree -- the payout is something like 12.5 cents on the dollar. With a max of 5 grand, it

takes a real dweeb to blow anything on a ticket. Of course, they are selling millions per week . . . . Innumeracy runs rampant.

Mike Beede, Secure Computing Technology Corp 1210 W. County Rd E, Suite 100,  
Arden Hills, MN 55112 (612) 482-7420

---

**✂ Re: Lottery ([RISKS-9.89](#))**

*Emmett Hogan <hogan@csl.sri.com>*

*Mon, 07 May 90 13:44:30 -0700*

This is true. If you win any lottery amount for which you must go to the lottery office to collect (usually \$1,000 and up) they will check you records for:

- 1) Outstanding Taxes Owed.
- 2) Gov't supported loans which are in arrears  
(i.e. delinquent or defaulted STUDENT loans)
- 3) Any fines (parking, traffic, etc) owed.
- 4) Basically any outstanding money owed to the gov't.  
(Provided it is in collections)

and take that out of your winnings. I had a friend who had won \$1,000 in the Virginia lottery but had several thousand dollars in delinquent student loans, so he had to find a very good friend, who didn't owe the gov't money, and whom he trusted ALOT to go pick up the money.

Emmett Hogan Computer Science Lab, SRI International

[Further contribution from david paul hoyt <YZE6041@vx.acs.umn.edu>  
steve@jhereg.Minnetech.MN.ORG (Steve Peterson).]

---

**✂ Risk of Unauthorized Access to TRW Credit Database**

*Larry Lippman <larry@kitty.UUCP>*

*8 May 90 14:41:50 EDT (Tue)*

Ever wonder how TRW access information gets "discovered"?

TRW dialup access is still notoriously unsecure, and any employee in the credit office of a legitimate TRW subscriber (like a major retail store) can obtain in a matter of minutes access information which would allow any third party with a PC to spoof the legitimate TRW subscriber.

During the 1970's when many TRW subscribers were still using ASR-33 teletype machines to access the TRW database, the lack of security was appalling. Typically, a TRW subscriber would encode credit request information for one or more customers while the ASR-33 was offline; i.e., they would punch a paper tape. The TRW access code (common to a local area) and subscriber identification number was encoded in the answerback drum of the ASR-33. The first part of the paper tape consisted of this punched information when the answerback was triggered by the operator entering a CTRL-E, which was the first

step in preparing the paper tape. A measly two-character "security check" was then entered by hand. This two-character "security check" often remained the same for the better part of a year. After the tape was prepared it was placed in the ASR-33 reader and the local access number dialed. Following printing of the reports, the paper tape was discarded - usually without regard to security. Anyone rummaging through a dumpster who got their hands on even ONE paper tape would obtain all the access information necessary to spoof the target store.

But wait... it gets *\*worse\**... The two-character "security check" code was also openly printed on any resultant credit report! And any customer who asked to see their credit report (a not unusual or unreasonable request, if made under appropriate circumstances), and who knew where to look could obtain the subscriber identification and security check code for the target store.

Short of implementing a hardware encryption or other security device whose physical presence is necessary and whose encryption and/or authentication keys cannot be readily extracted, the risk of unauthorized access to the TRW Credit Database will remain significant.

Larry Lippman @ Recognition Research Corp. a

---

### **✂ Unusual traffic light behaviour**

*<andyc@minster.york.ac.uk>*

*9 May 1990 08:59:37 GMT*

As I was driving through York last night, I came to a set of traffic lights which were red-amber (for non-British readers, the British traffic lights work on a sequence of red, red-amber, green, amber, red). A driver in front of us had stopped at these lights (which is slightly unusual, most UK drivers seem to take red-amber as meaning 'go', although you are supposed to wait until the lights go green). After waiting at the lights for twenty seconds or so, it became apparent that the lights weren't going to change (they normally stay red-green for 1.2 seconds, if my memory serves me correctly), so the driver drove on, and we followed him.

Traffic controllers in the UK are based around a microprocessor controlling up to 16 or 32 'phases' (i.e. different sets of lights). In addition to software protections, a hardware interlock is provided to ensure that no two conflicting phases go green at the same time. However there is only software preventing other failures. In York there is also a traffic control centre, which can alter traffic light timings, and other parameters (the controller software cannot, however, be altered).

A possible scenario of what happened is that the register containing the time of the red-amber state became altered from 6 to some larger time step (the timings go up in steps of 0.2 seconds). The implications of this are slightly worrying: green lights on one phase with red-amber on a conflicting phase.

The above information is based on my employment with a company who makes traffic controllers, and may be incorrect in places, but is mostly correct.

Andy Coombes, Department of Computer Science, University of York, Heslington,  
YORK

---

### **✂ High School Boy's Story was a Fake (Sharp Virus)**

*Yoshio Oyanagi <oyanagi@is.tsukuba.ac.jp>*

*Mon, 7 May 90 18:36:54+0900*

I posted a news about two kinds of virus Namba I and Namba II on Sharp X68000. During the long vacation of Japan (so called Golden Week, until May 6) the story of a high school boy about making the virus with forty people according to the request of a client turned to be a fake. Asahi Shinbun newspaper on its May 4 issue printed an apology for making trouble to many people with the unfounded story.

It remains a mystery who made the two viruses and how the game software was contaminated by them.

Yoshio Oyanagi (Univ. of Tsukuba)

---

### **✂ More about Sharp's Viri in Japan**

*Yoshio Oyanagi <oyanagi@is.tsukuba.ac.jp>*

*Thu, 10 May 90 19:28:13+0900*

Artdink Inc. is now distributing the vaccine against the virus which was contained in the simulation game software "FAR SIDE MOON". It says that the virus in question is attached to the battery backed-up area of the SRAM of X68000 and if the system is booted by a floppy without the protect seal, the floppy is contaminated. It is named "NX68K IPL V1.02". The effect of the virus is it will destroy the data on the floppy after July this year. This virus started to prevail among X68000 users last December.

Artdink started to sell "FAR SIDE MOON" for X68000 on April 13 (Friday !!!!!). 3200 sets have been sold before calling back due to the virus. Not all the articles are contaminated, only those in limited lots. This software consists of three floppies, among which only game disk is contaminated while system and data disks are not. If a user boots the dirty floppy according to the manual, the virus is not transferred to the SRAM.

The vaccine, named "DOCTOR" was written by the editorial office of the journal "Oh! X" for X68000 users. It initializes the SRAM and make it immune and it kills the virus on the floppy. However, it is effective only to two viri V1.02 and V1.05.

Yoshio Oyanagi (Univ. of Tsukuba)

---

### **✂ ARMY wants computer viruses for battlefield use (Gary McClelland)**

"Gary McClelland" <gmcclella@clipr.colorado.edu>

7 May 90 13:09:00 MDT

The Boulder, CO Sunday Camera for May 6, 1990 reports [in a box of "National Briefs" attributed to unnamed "Camera wire services"]

Army considers computer virus as weapon:

The U.S. Army is looking for help to develop the seeds of new-age germ warfare:

It wants business to help it turn computer "viruses" into military weapons. Experts predict the viruses, if successfully developed, could be used to wreak havoc on the increasing number of computers in the battlefield. The destructive computer programs, which have increasingly damaged commercial and research computer systems in the past four years, could be used to disrupt military communications, impede the control of weapons and feed misleading data to enemy commanders.

The viruses could also be used to alter the programming of crucial communications satellites serving combat units, the experts said. The Army is soliciting bids from small businesses to determine the feasibility of using computer viruses in warfare. And it is willing to pay as much as \$550,000 to a company that comes up with a plan for creating the programs -- and figures out how to use military radio systems to introduce them into enemy computers.

[No mention of a comparable RFP to protect the Army's computers against the same fate.]

Gary McClelland gmcclella@clipr.colorado.edu

[Also noted by jwm@stdc.jhuapl.edu (Jim Meritt)]

---

## **A-320 avionics malfunctions**

Vic Riley <riley@src.honeywell.com>

Tue, 8 May 90 15:18:02 CDT

An Associated Press story in the May 7 St. Paul Pioneer Press says that Northwest Airlines is having recurring problems with its A-320 flight control systems. "Northwest has sent pilots a bulletin advising them of possible problems following 'a recent series of events related to suspected failures' in the cockpit computer system." Northwest is reportedly involved in discussions with the FAA and Airbus to prevent and correct the problems. The rest of the report contains quotes and so forth maintaining that none of the failures has endangered passengers, and that such failures are normal "when you're breaking in an aircraft". No explanation of exactly what types of failures or anomalies have been observed.



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

**Volume 9: Issue 91**

**Sunday 13 May 1990**

## Contents

- [Hubble Telescope pointing in the wrong direction](#)  
[Raymond Chen](#)
- ["Feds Pull Plug On Hackers"](#)  
[James K. Huggins](#)
- [Airline booking cancellation](#)  
[Pete Mellor](#)
- [Simple tone dialler bypasses British Telecom charging](#)  
[Nigel Roberts](#)
- [Risks of caller identification](#)  
[David A. Honig](#)
- [Avoiding ANI by Dialing 1-900](#)  
[Gary McClelland](#)
- [Duplicate Mailings of RISKS 9.89 -- BITNET](#)  
[Emmett Hogan](#)
- [Re: Hazards of laser printers](#)  
[Paul DuBois](#)  
[Peter Jones](#)
- [IFIP Conference Call for Papers](#)  
[Rick Schlichting](#)
- [CALL FOR PAPERS: Computing and Ethics](#)  
[Donald Gotterbarn](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ***✂* Hubble Telescope pointing in the wrong direction**

*Raymond Chen* <[raymond@bosco.Berkeley.EDU](mailto:raymond@bosco.Berkeley.EDU)>

*Fri, 11 May 90 12:53:29 PDT*

[excerpted from the San Francisco Chronicle, 10 May 1990]

... Jean Olivier, NASA's deputy manager of the Hubble project, said that when they designed pointing instructions for the telescope, astronomers relied on star charts made in the 1950s. But the stars have moved since then from Earth's vantage point. The mistake was made when the scientists

factored in the extent of that movement.

They corrected in the wrong direction and "instead of subtracting it they added it or vice versa," Olivier said. ...

[end of excerpt]

However, I've heard that the Daily Telegraph attributed the miscalculation to programmer error; a programmer mistyped the addition as a subtraction.

I'm more likely to believe the Chronicle's report, as the media nowadays prefer to attribute errors to "computer error" if they can; otherwise they'll try to attribute it to "programmer error". Saying that the scientists messed up is much less exciting-sounding and doesn't sell as many papers.

--rjc

---

### ✂ "Feds Pull Plug On Hackers": Newspaper Article

*James K. Huggins <huggins@dip.eecs.umich.edu>*

*Fri, 11 May 90 12:26:08 -0400*

>EXCERPTED From The Detroit News, Thursday, May 10, 1990, Section B, p.1:

#### FEDS PULL PLUG ON HACKERS

Computer-fraud raid hits two homes in Michigan

By Joel J. Smith, Detroit News Staff Writer

Secret Service agents got a big surprise when they raided a Jackson-area home as part of an investigation of a nationwide computer credit card and telephone fraud scheme. They found a manual that details how almost anybody can use a computer to steal. It also describes how to avoid detection by federal agents. On Wednesday, James G. Huse, Jr., special agent in charge of the Secret Service office in Detroit, said the manual was discovered when his agents and Michigan State Police detectives broke into a home in Clark Lake, near Jackson, on Tuesday. Agents, who also raided a home in Temperance, Mich., near the Ohio border, confiscated thousands of dollars in computer equipment suspected of being used by computer buffs -- known as hackers -- in the scheme.

The raids were part of a national computer fraud investigation called Operation Sundevil in which 150 agents simultaneously executed 28 search warrants in 16 U.S. cities. Forty-two computer systems and 23,000 computer disks were seized across the country. The nationwide network reportedly has bilked phone companies of \$50 million. Huse said the Secret Service has evidence that computers in both of the Michigan homes were used to obtain merchandise with illegally obtained credit card numbers. He said long-distance telephone calls from the homes also were billed to unsuspecting third parties.

There were no arrests, because it was not known exactly who was using the computers at the homes. Huse also said there was no evidence that the suspects were working together. Rather, they probably were sharing information someone had put into a national computer "bulletin board". [...]

---

## ✂ Airline booking cancellation (Now there's a funny thing...!)

Pete Mellor <pm@cs.city.ac.uk>

Fri, 11 May 90 01:36:59 PDT

Narrative in a nutshell:

Requirement: Fly to Toulouse from London late on Sunday 6th May (but not too late to get a good French meal!). Install and check software for demo at workshop in 2 weeks' time. Return afternoon of Monday 7th May.

Implementation: Travel agent books Dan-Air flight. Sends tickets in folder with "6/5/90" scribbled on cover (no proper itinerary provided). Understand from secretary flight is 1430 from Gatwick.

Bug: Check ticket at 0530 Sunday morning. (Academic life isn't as relaxed as it used to be pre-Thatcher :-). Flight actually booked for 1430 Saturday 5th May. Ring travel agent in panic. Agent apologises for cock-up. Promises no problem: rebook flight for 1430 Sunday, flight nowhere near full. Grateful relief. Begin to feel sorry I woke his wife up so early.

Operation: Uneventful flight out. Nice dinner. Software works (!! :-). Arrive Toulouse airport for return flight.

Another bug: "You don't seem to be booked on this flight, monsieur! But I see that your ticket is valid. No problem! The flight is not full. We can book you a seat."

"But how the..."

"Mais oui! If you did not show up for the outward flight, your return booking would be automatically cancelled. But as it happens, we have spare seats, so do not worry!"

Diagnosis: Minor communications problem, aggravated by Dan-Air's natural assumption that someone who hadn't bothered to turn up to fly \*out\* to Toulouse wouldn't be turning up \*in\* Toulouse to fly \*back\*.

But wait...

In-depth diagnosis (Courtesy of Ralph Adam, offering consultancy at the usual City University rate in the Saddlers' Bar, Thursday 11th May, late):

Dan-Air use the Texas Air Services airline booking system "System 1". (This is one of the 'big four', all based in the US, and is owned by US Airlines.) Built into this database is a requirement that a return flight be reconfirmed after departure on the outward leg of the journey. The reason is to prevent passengers in the US buying a return ticket (cheaper than a single in some cases) and using the return half only. My problem on return had nothing to do with Dan-Air. It was a side-effect of an attempt to close a loophole in the ticket price structure of various US airlines.

The database is physically situated in the US. On-line access for seat booking

is, well, on-line. Any other information retrieval requires 3 to 4 weeks of bureaucratic delay. If the flight had been full, if I had been stuck in Toulouse for a couple of days, and if I had raised hell (Oh, no! Not another hot oysters in champagne and steak tartare at the Brasserie des Beaux Arts! 'Allo, 'allo! C'est moi encore! Il n'y avait plus de places sur l'avion. Ah, ton mari! Quelle bonne surprise! :-), it might have taken a month to answer my query about why the return flight had been cancelled (assuming the travel agent and airline didn't already know!).

I am assured by Ralph that this sort of thing is old hat to veteran readers of RISKS, but if anyone is interested in the economics of airline booking systems, the following should be a good read:

Adam R.: "A Licence to Steal", J. of Information Science, Iss. 2, 1990

Peter Mellor, Centre for Software Reliability, City University,  
Northampton Square, London EC1V 0HB Tel.: +44 (0)71-253-4399 Ext. 4162/3/1

---

### **✶ Simple tone dialler bypasses British Telecom charging**

*Nigel Roberts <roberts@egse.enet.dec.com>*

*Thu, 10 May 90 08:09:11 PDT*

The following is extracted from a front page article in today's DAILY MIRROR.  
The 2 inch high headline reads:

F R E E P H O N E  
T H E W O R L D

"BRITISH TELECOM is being conned out of millions by fiddlers making free international calls ... using a BT gadget.

Shocked Telecom chiefs secretly tried to withdraw the GBP 9.95 "magic box" which is supposed to be used with phone answering machines -- a month ago.

But the DAILY MIRROR can disclose they are still on sale in BT stores."

...

"And there is a thriving black market for them on street corners and in pubs where they are changing hands for up to GBP 1000. The 3in x 2in device, known as a remote interrogator, is designed to enable people to phone home and pick up messages from their answering machines. But cheats have discovered that by using it in some phone boxes and pressing two vital numbers, they can call anywhere in Britain or the world without charge."

---

There's a full colour photograph of the "device" on the front-page. It appears to be a simple 12-key DTMF tone dialler. I seriously doubt that they are changing hands for GBP 1000, but if they are, I have this bridge that

their purchasers might also be interested in ....

The risk management (or utter lack of it) in this case is so obvious that I'll refrain from adding any further comment.

Nigel Roberts.

Tel: +44 860 57 860 0

---

### **✂ risks of caller identification**

*"David A. Honig" <honig@bonnie.ICS.UCI.EDU>  
Thu, 10 May 90 09:48:33 -0700*

I recently had an unpleasant taste of the disadvantages of the caller identification that may be more widespread soon.

A few weeks ago I called the university police's business line from my office phone and asked a few minutes of questions about how to find out about outstanding warrants (I had heard of someone getting arrested while renewing his driver's licence). I informed the officer that I spoke with that this was entirely moot. After receiving my replies, I thought that was the end of it.

Thus you can imagine my surprise and annoyance to find that two uniformed, armed officers and their sergeant came to my workplace (having located that using the campus centre's caller-id ability on phones with appropriate displays), spoke with my coworkers, knocked on my office door, and via surprise and intimidation verified my ID. This permitted them to run a warrant check on me. I was clean, which was no surprise to me. They skulked away shortly thereafter.

Conversations with the chief of police indicated that the rather zealous instigating officer's behavior was within "acceptable" bounds, and if you raise "enough" suspicion (on a slow day?), this constitutes justification for nosing about your workplace.

The RISK is that the officer wouldn't have been able to easily trace the number except for the abilities of the private exchange.

---

### **✂ Avoiding ANI by Dialing 1-900 (Gary McClelland)**

*"Gary McClelland" <gmcclella@clpr.colorado.edu>  
12 May 90 11:42:00 MDT*

Summary of report on All Things Considered (NPR), Friday, May 11, 1990:

Private Lines, Inc. of Beverly Hills provides a telephone service for those wanting to avoid automatic number identification. You simply call a 900 number which then lets you call out through Private Lines WATS numbers. ANI at the receiving end of course then displays only the Beverly Hills number of Private Lines. NPR interviewed president of Private Lines who defended need for such a service. He of course said that the service was not intended to

help obscene callers and their rates would make obscene calling through Private Lines a very expensive habit (\$2/minute, I think). (NPR noted that ANI had already resulted in several arrests of obscene callers in the Atlantic Southern area where ANI is heavily promoted for that purpose.) He cited the following legitimate reasons for avoiding ANI and any billing record of the numbers called. (1) Boss is quietly working on a merger deal and doesn't want secretaries and accountants in the firm noticing a sudden increase in calls to a particular other firm. (2) Separated spouse wants to call kids but doesn't want spouse to know from where he or she is calling. (3) Caller to crisis line or crime tip line wants to guarantee anonymity.

Gary McClelland gmcclella@clipr.colorado.edu

---

### ✂ Duplicate Mailings of [RISKS 9.89](#)

*Emmett Hogan <hogan@csl.sri.com>*

*Mon, 07 May 90 14:17:49 -0700*

[As root@csl,] I received several replies from people who got two copies of [RISKS 9.89](#). All these people have one thing in common....BITNET !!

I have asked these people for the headers of the RISKS digests in hopes of narrowing it down to one listserv machine.

I will keep you up to date on my findings,

-E-

[The above problem was clearly a BITNET problem. Later news indicates the surprise discovery of a lurking CHRON problem that forced another pass over a random sublist when a time-out occurred. The resulting cleanup -- without changes to our sendmail -- has resulted in no duplicate mailing problems on our end for the last four four issues. Perhaps our main woes are over. Stay tuned for details. PGN]

---

### ✂ Re: Hazards of laser printers ([RISKS-9.89](#))

*bin@primate.wisc.edu (Brain in Neutral) <Paul DuBois>*

*7 May 90 19:12:59 GMT*

New England Journal of Medicine, 3 May 1990, has a letter to the editor, p. 1323, titled "Laser-printer rhinitis".

---

### ✂ Photocopier hazards

*Peter Jones <MAINT@UQAM.bitnet>*

*Sat, 12 May 90 07:11:55 EDT*

The purpose of this posting is to thank those who recently posted regarding the possible environmental hazards of photocopiers -- and to invite them to repost

to the SAFETY list at UVMVM!

Peter Jones (514)-987-3542

---

## **✂ IFIP Conference Call for Papers**

*"Rick Schlichting" <rick@cs.arizona.edu>*

*Sun, 6 May 90 22:38:26 MST*

**\*\*CALL FOR PAPERS\*\***

Second IFIP Working Conference on  
DEPENDABLE COMPUTING FOR CRITICAL APPLICATIONS  
Can we rely on computers?

Hotel Park Tucson, Tucson, Arizona, USA  
February 18-20, 1991

Organized by

IFIP Working Group 10.4 on Dependable Computing and Fault Tolerance

This is the second Working Conference on this topic, following a successful initial conference held in August, 1989, on the campus of the University of California at Santa Barbara (USA). As evidenced by papers that were presented and discussed at that meeting, critical applications of computing systems are concerned with differing service properties, relating to both the nature of proper service and the system's ability to deliver it. These include thresholds of performance and real-time responsiveness that demark loss of proper service (failure), continuity of proper service, ability to avoid catastrophic failures, and prevention of deliberate privacy intrusions. The notion of dependability, defined as the trustworthiness of computer service such that reliance can justifiably be placed on this service, enables these various concerns to be subsumed within a single conceptual framework. Dependability thus includes as special cases such attributes as reliability, availability, safety, and security. In keeping with the goals of the previous conference, the aim of this meeting is to encourage further integration of theory, techniques, and tools for specifying, designing, implementing, assessing, validating, operating, and maintaining computer systems that are dependable in the broad sense. Of particular, but not exclusive, interest are presentations that address combinations of dependability attributes, e.g., safety and security, through studies of either a theoretical or an applied nature.

Submitting a Paper: Five copies (in English) of original work should be submitted by August 13, 1990, to the Program Chair:

John F. Meyer, EECS Department, 2114B EECS Bldg.,  
The University of Michigan, Ann Arbor, MI 48109-2122, USA  
Tel: +(1) 313 763 0037 Fax: +(1) 313 763 4617  
E-mail: jfm@eecs.umich.edu

Papers should be limited to 6000 words, full page figures being counted as 300 words. Each paper should include a short abstract and a list of keywords indicating subject classification.

Important Dates:

Submission deadline: August 13, 1990

Acceptance notification: November 25, 1990

Camera-ready copy due: January 14, 1991

General Chair

R.D. Schlichting

The University of Arizona, USA

Vice-General Chair

J.J. Quisquater

Philips Research, Belgium

Program Committee

J. Abraham (USA), A. Costes (Fr.), M.C. Gaudel (Fr.), V. Gligor (USA),

J. Goldberg (USA), D. Gollmann (FRG), G. Hagelin (Sweden),

H. Ihara (Japan), H. Kopetz (Aus.), J. Lala (USA), C. Landwehr (USA),

G. Le Lann (Fr.), J. McDermid (UK), M. Morganti (Italy),

J.M. Rata (Fr.), D. Rennels (USA), J. Rushby (USA), E. Schmitter (FRG),

S. Shrivastava (UK), D. Siewiorek (USA), L. Simoncini (Italy),

R. Turn (USA), U. Voges (FRG)

---

**CALL FOR PAPERS: Computing and Ethics**

<gotterbarn@wsuiar.UUCP>

10 May 90 15:32:17 CDT

The \*Journal Of Systems and Software\* is preparing a special issue on Computing and Ethics. Although the major emphasis will be ethical issues faced by the Computing Professional, other subjects will be considered.

Please send your papers by July 1, 1990 to:

Donald Gotterbarn

The Wichita State University

Computer Science, Box 83

Wichita, KS 67208

Send questions by email to:

gotterbarn@wsuiar.wsu.UKans.EDU, gotterbarn@twsuvax.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 9: Issue 92

Thursday 17 May 1990

## Contents

- [Army chafes under Congress' robot weapons ban](#)  
[Jon Jacky](#)
- [Re: \[London\] Tube train leaves ... without its driver](#)  
[Gavin Oddy](#)
- [Re: First Hubble Images Delayed To Conduct Focusing Tests](#)  
[Karl Lehenbauer](#)
- [ANI for the criminal as well as the private citizen](#)  
[Brad Templeton](#)
- [Computer Virus Solicitation](#)  
[Andy Warinner](#)
- [Feds Pull Plug On Hackers](#)  
[Bob Sutterfield](#)  
[Rick Clark](#)
- [Re: Military Viruses](#)  
[Jim Vavrina via David Brierley](#)
- [Re: Magnetic ID cards for all Israeli citizens](#)  
[Amos Shapir](#)
- [Risks of Laser Printouts](#)  
[David Tarabar](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✉ [Army chafes under Congress' robot weapons ban](#)

*Jon Jacky <JON@GAFFER.RAD.WASHINGTON.EDU>  
Tue, 15 May 1990 11:48:19 PDT*

The following dialog occurred in hearings before the U.S. Congress' House Appropriations Committee in March, 1989:

Mr. (Martin Olav) Sabo (Rep. from Minnesota): I am curious about robotics and what you see as its future. I forget particular programs as we go along, but I was involved in discussions last year with the other body on a program. They seemed very negative on robotics research, which struck me as something we should be aggressively pursuing.

Mr. (George T.) Singley (Director of Army Research and Technology): We have a problem about restrictions placed on us, but not on the Marine Corps, relative to Army robotic vehicles, so our robotics program does not include weapons on unmanned ground vehicles. ...

Mr. (John P.) Murtha (Rep. from Pennsylvania): Restrictions by whom?

Mr. Singley: By Congress.

Mr. Murtha: We put restrictions ---

(Lt.) General (Donald S.) Pihl (Deputy to the Assistant Secretary of the Army for R&D): To put a weapon on a robot vehicle. We were told to restrict our robotic vehicle work to reconnaissance and surveillance.

Mr. Sabo: Generated by the other body?

General Pihl: Yes, sir.

Mr. Murtha: Staff tells me that in the conference last year, that the Senate wanted to go forward with robotics research and make sure you got the bugs worked out before you started working out systems with weapons; does that make sense?

General Pihl: Yes, sir. It is a logical approach as long as you don't have a restriction on weaponizing the unmanned ground vehicle forever.

Mr. Murtha: What would you recommend we do this year?

General Pihl: Sir, I think you should allow the Army to proceed with a roboticized look at a ground-launched Hellfire system in conjunction with the Marine Corps. I think that would be a good thing to do.

Mr. Murtha: Let's move on ... [ to other topics...]

The reference is: Department of Defense Appropriations for 1990, Hearings Before a Subcommittee of the Committee on Appropriations, House of Representatives, One Hundred First Congress, First Session, Subcommittee on the Department of Defense. (Superintendent of Documents "Su Docs" number: YkAp6/1 D36/5/990/pt. 7), pages 132-133.

Jonathan Jacky

University of Washington

---

### [London] Tube train leaves ... without its driver

*gco <gco@gec-mrc.co.uk>  
16 May 1990 10:43:49-BST*

Regarding Stephen Page's contribution of 16 Apr 90...

This incident was used as an example at a colloquium on Systems Engineering

which I attended yesterday, where it was referred to as the handbag problem. It seems that the system designers had succeeded in optimising the controls on the train to two buttons: one to close the doors and another to start the train. An interlock prevented the train starting until the doors were indeed closed.

The driver of the train in question decided to optimise the system design further (to one button) by taping the second of these buttons permanently down so that (s)he only had to press the button to close the doors. The train would then go once they had closed as the second button was always depressed. This worked satisfactorily until a handbag became trapped in the doors and, as reported, the driver (following his training) went to the doors and prised them apart, freeing the handbag, allowing the doors to close and completing the set of events required for the train to depart (without the driver).

The driver had failed to realise and/or take into account that the second button (for making the train go) was implementing the requirement that the driver should be in the cab before the train could go.

In retrospect, perhaps the action of depressing the second button (rather than the state of depression) should have been required to start the train; but such statements are easy to make with hindsight.

Gavin Oddy

---

### **✂ First Hubble Images Delayed To Conduct Focusing Tests ([RISKS-9.91](#))**

*Karl Lehenbauer <karl@sugar.hackercorp.com>*

*16 May 90 08:09:09 CDT (Wed)*

A brief report in Aviation Week (May 14, 1990, page 42) says that the first test pictures from the Hubble Space Telescope are being delayed until ground controllers can conduct optical system focusing exercises.

Hubble engineers have been trying to determine why the telescope's guidance sensors were not properly locking onto "guide stars." They have since determined that there was an error in the pointing data provided to the telescope by the Space Telescope Science Institute.

The error occurred because someone several years ago inserted a plus sign instead of a minus sign in a computer program being prepared to aid in early telescope checkout.

The star data being used came from a 1954 star survey. Engineers realized the Earth's precession in relation to the 30-year-old star data would have to be accounted for in the Hubble checkout data.

The precession equated to an 18 arc minute reduction in the coordinates of the star field, but a programmer accidentally added 18 arc minutes instead.

That resulted in the telescope being a full 0.5 degrees off target in the initial pattern recognition tests.

Engineers are also working to solve a .1 Hz jitter problem the telescope has for 20 to 30 minutes whenever it passes from the dark side of its orbit into sunlight. They believe the problem is related to thermal effects from the telescope's solar arrays, but they doubt the problem will seriously affect the telescope's mission.

---

## ✂ ANI for the criminal as well as the private citizen

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

*Mon, 7 May 90 16:53:53 EDT*

The following article appeared in clari.tw.telecom, and I thought it was appropriate for RISKS. Reprinted with permission, for use within the RISKS digest only. (For more information on the ClariNet news service, write to info@clarinet.com.) While I have no sympathy for drug dealers, I don't feel that this is a negative aspect of ANI. I myself would like to know if a call comes from the Police, Government or other enforcement agency, even if I have done nothing wrong.

>Subject: Drug dealers find uses for Caller ID equipment

>Keywords: illegal drugs, legal, telecom, media

BALTIMORE (UPI) -- Like telephone pagers and mobile cellular phones before it, the latest in telephone technology, the Caller ID machine, is proving a valuable tool for drug traffickers.

Drug enforcement officials in Baltimore say that the Caller ID machines are starting to turn up in drug raids, which may be proof that once again, dealers find benefits in the communications revolution.

Caller ID, which has been on the market for several months, has been advertised as a means of crime prevention -- giving people receiving harrassing calls a chance to see the phone number the call is being made from even before they pick up the receiver.

But such a service apparently also means that drug dealers, eager to protect their business from undercover police operations, can screen the phone calls they receive and refuse to answer a suspicious call.

"It's frightening," said Assistant U.S. Attorney Katharine Armentrout, who has seen Caller ID equipment confiscated in drug raids.

Even though an undercover police operation would have a different phone number than a police station, dealers could worry about calls from an unfamiliar exchange.

"The question then becomes, 'Where are you calling from?'" a federal surveillance expert told the Baltimore Sun, in an article printed in Sunday's editions. "Or more to the point, 'Why aren't you calling me from your usual pay phone?'"

The problem has been much the same with other recent progress made in the telecommunications industry. Pagers were developed for doctors, lawyers and other professionals, but dealers have found them useful. And mobile cellular telephones have created a myriad of surveillance problems for police tracking drug dealers.

Phone company officials in the Baltimore and Washington areas say they are looking for ways to solve the problems law enforcement agencies have with the Caller ID equipment.

"We're committed to finding solutions," said Al Burman, a spokesman for C&P Telephone Co. "There are a number of things that can be done that aren't being done."

One solution may be to block certain numbers from being picked up by the machines. Burman said there are enough numbers in the Baltimore area not linked to the Caller ID system currently to avoid arousing any suspicions.

Police officials pointed out, however, that as more telephone numbers become linked with the system, blocked numbers will become more suspicious to traffickers.

Brad Templeton, ClariNet Communications Corp. -- Waterloo, Ontario 519/884-7473

---

### **Computer Virus Solicitation**

*Andy Warinner <andy@tasha.UUCP>*

*11 May 90 11:54:50 CDT (Fri)*

There has been some discussion in the media and the net lately about the Department of Defense sponsoring research into computer viruses. Here is the solicitation in question. It is part of the government's Small Business Innovative Research (SBIR) program. The SBIR program is designed to help small companies develop advanced technologies. Up to \$50,000 can be awarded in Phase I and up to \$500,000 can be awarded in Phase II.

Title: Computer Virus Electronic Counter Measure (ECM)

Objective: The objective shall be to determine the potential for using "computer viruses" as an ECM technique against generic military communications systems/nets and analyzing its effects on various subsystem components.

Description: The purpose of this research shall be to investigate potential use of computer viruses to achieve traditional communications ECM effects in targeted communications systems. These effects can include data (information) disruption, denial, and deception, but other effects should also be researched such as effects on executable code in processors, memory, storage management, etc. Research in effective methods or strategies to remotely introduce such viruses shall also be conducted. Efforts in this area should be focused on RF atmospheric signal transmission such as performed in tactical military data communications.

Phase I: Phase I shall analyze the feasibility of using viruses as an ECM technique. Analysis shall include validity studies of the concept, types of viruses suitable to be employed in this concept, strategies for virus injection, and/or simulated predictions of effects. Phase I shall culminate with the submission of a final report that details the above analysis and outlines a method that can validate the concept.

Phase II: Based on analysis performed under Phase I, develop a demonstration method that can validate the virus ECM concept and demonstrate various ECM techniques or strategies. Phase II shall culminate with this demonstration and a final report describing demonstration methodology, results, and analysis of effects compared with predicted effects from the Phase I effort. The final report shall also summarize or make conclusions as to the future potential of using virus ECM techniques or strategies.

Andrew Warinner, GIST, Inc.

---

**✂ Feds Pull Plug On Hackers (Huggins, [RISKS-9.91](#))**

*Bob Sutterfield <bob@MorningStar.Com>*

*Tue, 15 May 90 14:52:17 GMT*

...[the Secret Service agent] also said there was no evidence that the suspects were working together. Rather, they probably were sharing information someone had put into a national computer "bulletin board". [...]

Does our law enforcement community really think that "working together" requires physical presence? Don't they recognize that sharing information via a cracker bulletin board is collaboration? Isn't this the whole point of a computer security case?

---

**✂ Re: "Feds Pull Plug On Hackers" ([RISKS-9.91](#))**

*~XT6561210~Rick Clark~C24~H15~6011~ <rbc@cuuxb.ATT.COM>*

*15 May 90 14:13:31 GMT*

Boy, do I hate sensationalism in journalism.

Does anyone besides me find it difficult to believe these 42 computers ran up over a million dollars apiece in unpaid phone time? You *could* do it in a month or two if you had connect time 24 hours a day (very) long distance, or a couple hours a day for two years. So, its possible, but I don't believe it for all 42 systems.

It's also pretty colorful to refer to a "nationwide network" of people for which "there was no evidence that [they] were working together".

Richard B. Clark, Lisle, IL

---

**✂ Re: Military Viruses [From VIRUS-L vol 3 issue 93]**

*<davidbrierley@lynx.northeastern.edu>*

*Sun, 13 May 90 21:16:22 EST*

Date: Thu, 10 May 90 13:43:15 -0500

From: "Mr. J. Vavrina" <SDSV@MELPAR-EMH1.ARMY.MIL>  
Subject: RE: Military Viruses (THE FACTS)

After reading, in astonishment, Nick DiGionanni's input regarding Military Viruses, (VIRUS-L 3-90 8 May 90) the phone lines were burning up from my office to the DOD Information Systems Security Management Office checking on the validity of the story. No one had even heard of such a project being undertaken. A few more phone calls later generated a FAX to my desk of an article from the Philadelphia Inquirer titled, "Army Searches for new weapon: Computer Virus", written by Rory J. O'Connor. The article quoted an individual as being the administrator of the project. Now the hunt started to locate her. Within a few hours I had her on the phone. Needless to say, the reporter identified himself as a small businessman and was interested in this program. The information given to him was completely turn around so that he could make a big story out of nothing.

HERE ARE THE FACTS: The Department of Defense published a booklet titled, "PROGRAM SOLICITATION 90.2 FY-1990 SMALL BUSINESS INNOVATION RESEARCH (SBIR) PROGRAM". On page 45 can be found the following:  
A90-217 TITLE: Computer Virus Electronic Counter Measure (ECM)  
CATEGORY: Exploratory Development  
OBJECTIVE: The objective shall be to determine the potential for using "computer viruses" as an ECM technique against generic military communications systems/nets. The goal shall be to determine the feasibility of remotely introducing a virus into a system/net and analyzing its effects on various subsystem components.  
DESCRIPTION: The purpose of this research shall be to investigate potential use of computer viruses to achieve traditional communications ECM effects in targeted communications systems. These effects can include data (information) disruption, denial, and deception, but other effects should also be researched such as executable code in processors, memory storage management, etc. Research in effective methods or strategies to remotely introduce such viruses shall also be conducted. Efforts in this area should be focused on RF atmospheric signal transmission such as performed in tactical military data communications.

It continues on to explain what needs to be accomplished in each phase.

As you can see, this is nothing more than a feasibility study to answer the famous "WHAT IF WE COULD ??????" question. Admittedly, myself and many of my colleagues are quite surprised that something of this nature would be put on the streets for research and not using the expertise internally available.

Jim Vavrina, Computer Security Specialist, Intelligence and Security Division,  
US Army Information Systems Software Center.  
Comm 703-355-0010/0011 AV 345-0010-0011

---

**✉ Re: Magnetic ID cards for all Israeli citizens**

*Amos Shapir <amos@taux01.nsc.com>*

14 May 90 15:11:26 GMT

(This is a repost from talk.politics.mideast, originally posted by HANK@BARILVM.BITNET (Hank Nussbacher))

>From the Jerusalem Post, May 7, 1990:

>

>The Director-General of the Ministry of the Interior announced yesterday >that within 3 months all Israeli citizens will be issued magnetic id >cards. He stated that with the new cards it will take only 10 minutes >to issue a new passport and that all future elections will no longer have >manual balloting.

[End quote]

Though the current method of balloting is very cumbersome and wasteful, I wonder if anyone at the Ministry of the Interior ever read comp.risks...

Amos Shapir, National Semiconductor (Israel) P.O.B. 3007, Herzlia 46104, Israel

---

### ✂ Risks of Laser Printouts (More on [RISKS-9.89](#))

David Tarabar <dtarabar@hstbme.mit.edu>

Thu, 17 May 90 09:47:12 -0400

In the New England Journal of Medicine dated May 3, 1990, there is a letter to the editor titled: 'Laser-Printer Rhinitis' on page 1323. In this letter, the authors report on a single recent patient case.

"A 51-year-old man was seen for nasal and systemic symptoms that developed repeatedly after he handled documents from a laser printer. He had worked for the same insurance company for 21, years spending an average of three to four hours per day on computer and clerical work. In April of 1987 a new computer system with a laser printer was installed at his work station. During the next six weeks he had increasing intermittent nasal congestion, with a burning sensation on his skin, headache, and diffuse retrosternal and epigastric discomfort. He had no history of asthma, allergies, hay fever or eczema, although his mother did." ...

"Two substance-specific challenges were performed, each preceded and followed by " [a computerized test] "On one occasion he shuffled laser-printed paper for 10 minutes, when nasal and other symptoms developed. The " [test] "demonstrated an increase of more than fourfold in nasal airflow resistance." [The second test demonstrated a three-fold increase in nasal airflow resistance when sitting next to an operating laser printer.]



Search RISKS using [swish-e](#)

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





Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 9: Issue 93

Monday 21 May 1990

## Contents

- [Stamford CT 18-hour telephone switch outage affects 27,000 lines](#)  
[PGN](#)
- [Irrational and nonvaedictory reasoning](#)  
[PGN](#)
- [Crackdown on 1-900-STOPPER?](#)  
[John M. Sulak](#)
- [P.T.U.U.I.](#)  
[Robert Hardy](#)  
[PGN](#)
- [Military Computer Virus Contract](#)  
[Rory J. O'Connor](#)
- [Risks of Laser Printouts](#)  
[Simson L. Garfinkel](#)
- [Directions and Implications of Advanced Computing, DIAC-90](#)  
[Rodney Hoffman](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **Stamford CT 18-hour telephone switch outage affects 27,000 lines**

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

Mon, 21 May 1990 18:10:52 PDT

At 2:42am on Thursday, 17 May, a Number 1A ESS switch (vintage 1973) in Stamford, Connecticut, broke down and for 18 hours blocked all residential and most business local calls (affecting 27,000 subscribers in exchanges 324, 326, 348, 351, 356, 358, 896, 964, 965, 969, 977, 979). (The same switch had broken down on 19-20 December 1985 for five hours, affecting 34,000 subscribers. Two such outages on the same switch is a very rare occurrence indeed.)

The outage occurred while technicians were doing routine maintenance to update the database of phones served by that switch (12 of Stamford's 17 exchanges). The switch computer rejected the update and shut itself down. The backup system also failed. The eventual return to service followed extensive remote diagnostics from the AT&T Technology Center in Indian Hill, Illinois. However,

the cause still remains unknown as of this afternoon (Monday).

[Source: three articles by Seth Amgott in The Advocate, Stamford CT, 18 and 19 May 1990, plus phone conversations.]

---

### **✶ Irrational and nonvaledictory reasoning**

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

*Mon, 21 May 1990 8:40:48 PDT*

In a masterpiece of overendowing mathematical precision, the UPI reported that East Lake High School in north Pinellas County, Florida, had computed the grade-point averages of three graduating seniors as 4.2857142. The headline "Scholastic Tie -- to the Seventh Decimal" suggests that no one along the way recognized 4 and two sevenths in disguise. Straight A records at that.

[Source: UPI item in the San Francisco Chronicle, 19 May 1990]

---

### **✶ Crackdown on anonymous 1-900 services? (Re: McClelland, [RISKS-9.91](#))**

*John M. Sulak <sulak@ge-dab.ge.com>*

*18 May 90 16:59:19 GMT*

This morning CNN had a story on the federal government in the US and how they plan to 'crackdown' on 1-900 toll phone services. One such service, 1-900-STOPPER was said to allow callers to make unidentified phone calls. Of course, the callers to 1-900 could be identified by the government by date and time, but it would require a court order or consent of the 1-900 company.

[... whose entire reason for existence is providing the service of anonymity/nonidentifiability! PGN]

---

### **✶ P.T.U.U.I.**

*Robert Hardy <a195@mindlink.UUCP>*

*Sat May 19 16:29:06 1990*

Announcing the formation of P.T.U.U.I.  
(the Programmers and Technical Underdogs Union International)

This organization was formed in response to the alarming proliferation of flaky employers.

Have you ever poured your heart and soul into an exciting project only to have the company go under the day its ready for market?

Have any of your previous employers pulled a 'Midnight Move'?

Have you worked diligently until the end of the month only to find the payroll

isn't covered?

Have you ever given your `Life's Work' to an employer only to have it stolen and marketed behind your back?

We invite you to share your experiences and to co-operate in identifying and disseminating the names of `non-professional' employers.

If one of our members has a bad experience, we would like to make it difficult if not impossible to find a competent replacement.

We would like to act as an `Ombudsman' to mediate disputes.

This group is open to all competent `Hardware' and `Software' independent contractors.

Reply via E-Mail to MindLink BBS: 1-604-576-1214

(195) Robert Hardy

PaNorAmA BBS: 1-604-281-1082

or 1-604-271-3098

Robert Hardy

USENET :

uunet!van-bc!rsoft!mindlink!RobertHardy

or Write to

P.T.U.U.I., 2994 Vincent St., Port Coquitlam, BC, V3B 5N2 Canada

---

### **✂ P.T.U.U.I. to you, too (thanks, Tom Lehrer!)**

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

*Mon, 21 May 1990 18:10:52 PDT*

P.T.U.U.I. reminds me of Tom Lehrer's ``Subway Song'', written while he was riding the Boston subway in the late 1940s or very early 1950s, but unfortunately never recorded. Particularly for those who know and love the `T', I recite it from memory (it is sung to the tune of ``Mother''), with apologies to Tom if I didn't remember it correctly, and apologies in advance to those purists who think it is irrelevant to RISKS. (Indeed, it is much too relevant to the foregoing contribution NOT to be included.) Cheers! PGN

H is for my alma mater, Harvard,  
C is Central, next upon the line,  
K is for the cosy Kendall Station,  
C is Charles, across the foamy brine,

P is Park Street, Boston's busy center,  
W is Washington, you see,

Put them all together, they spell HCKC PW, [sung with great emphasis]  
And that's just what Boston means to me.

---

### ✂ **Military Computer Virus Contract ([RISKS-9.92](#))**

*Rory J. O'Connor <rjoconnor@cdp.uucp>  
Sun, 20 May 90 14:25:39 PDT*

I'm the reporter at the San Jose Mercury News who wrote the story on the Army's SBIR proposal regarding computer viruses. I feel I must respond to the charge made by Mr. Jim Vavrina of the Army Information Systems Software Center that I mis-identified myself while researching the story. That assertion is false.

At all times, as is standard practice among professional journalists, I made it clear to everyone I called or interviewed that I was a newspaper reporter working on a story about this proposal. When I reached a woman named Joyce Crisci at Ft. Monmouth, NJ, who identified herself as the project administrator, I identified myself as a reporter. When she attempted to tell me how to apply for the available funds, I felt she might have failed to understand that, so I again told her I was a reporter working on a story for my newspaper. She then answered most of my questions, but made it clear she would not discuss any technical details nor provide me with the names of the engineers who had written the project. The reason, she said, was that if such information appeared in my story, it could prejudice the bidding process.

Indeed, at the conclusion of our interview, she verified the spelling of her name and gave me her (rather complicated) mailing address and requested I send her a copy of the article when it appeared in the newspaper.

I'm sorry Mr. Vavrina never called me to ask my side of the story about this interview. If Mr. Vavrina thinks my story about the virus was in some way factually incorrect, or did not fully describe the Army's project or reasoning, I'd be happy to talk to him about it. I can be reached at (408) 920-5019, or at MCI Mail mailbox 361-2192, or at the San Jose Mercury News, 750 Ridder Park Drive, San Jose, CA 95190. Anyone else who would like to discuss this story, or the topic of computer viruses in general, may also contact me there.

Rory J. O'Connor, Computing Editor, San Jose Mercury News

---

### ✂ **Risks of Laser Printouts ([RISKS-9.89,91,92](#))**

*Simson L. Garfinkel <simsong@next.cambridge.ma.us>  
Sun, 20 May 90 12:26:45 EDT*

Not very surprising, considering that laser printers pump out gobs of ozone.

The old DEC LN03 laser printer had an ozone filter on it that was supposed to be replaced at regular intervals. The ozone filter consisted of a granulated carbon filter. But this is the only laser printer that I have ever seen with such a filter.

simson

---

## **Conference: Directions and Implications of Advanced Computing**

*Rodney Hoffman <Hoffman.ElSegundo@Xerox.com>*

*18 May 90 13:24:18 PDT (Friday)*

Here's the program and registration information for a conference of interest, presented by Computer Professionals for Social Responsibility and co-sponsored by several other organizations:

Computer Professionals for Social Responsibility  
DIAC-90 SYMPOSIUM  
Directions and Implications of Advanced Computing  
July 28, 1990

Computer technology significantly affects most segments of society, including education, business, medicine, and the military. Current and emerging computer technology will exert strong influences on our lives, in areas ranging from work to civil liberties. The DIAC symposium considers these influences in a broad social context - ethical, economic, political - as well as a technical context seeking to address directly the relationship between technology and policy.

Gutman Conference Center / Monroe C. Gutman Library  
6 Appian Way Cambridge, Massachusetts

KEYNOTE ADDRESS: Dr. Michael Rabin, Computer Security and Privacy

Computer security is essential not just for the protection of valuable assets but also for safeguarding privacy. To this end technical tools are needed for correctly specifying who will access what personal data and for enforcing and monitoring the specified regime. These new technical tools as well as a new legal framework for defining the status of personal data will be presented.

Michael Rabin is a Turing Award winner who is T.J. Watson Sr. Professor of Computer Science at Harvard. He teaches and conducts research in the fields of computer algorithms and computer security.

### PAPERS

Rob Kling, "Four Genres of Social Analyses of Computerization"

Paul Resnick and Mel King, "The Rainbow Pages - Building Community with Voice Technology"

Chris Hables Gray, "AI at War: A Preliminary Analysis of the Aegis System in Combat"

Hank Bromley, "Thinking about Computers and Schools, A Skeptical View"

Sue Stafford, "Software for the Detection of Code Abuse - Answers and Issues"

Judith Perrolle, Glenn Pierce, Michele Eayrs, A. Gilbert, Nightingale Rukuba,  
"The Effects of Computer Models of Global Warming on Regional Environmental  
Policies in East Africa and Southeast Asia"

Nance Goldstein, "Software R&D in the Department of Defense in the 1980s:  
Institutional Resistance to the Demand of New Information Technology"

Doris Schoenhoff, "Language, Logic and Expertise: The Human Interface of Expert  
Systems"

David Durlach, "Affectionate Technology"

Joel Wolfson, "A Conduct Code: An Ethics Code with Bite"

Harold Sackman, "Developing an International Participative Code of Computer  
Ethics"

Natalie Dandekar, "Moral Issues Involved in Protecting Computer Software as  
Intellectual Property"

David Hakken, "Machine-, Human-, or Culture-centered Computing? A View from  
the Trenches"

PANEL DISCUSSION: Virtual Reality: What Does it Really Mean?

Co-Sponsored by American Association for Artificial Intelligence, American  
Philosophical Association, Boston Computer Society, Harvard University Science,  
Technology and Public Policy, MIT Science, Technology and Society Dept. in  
cooperation with ACM SIGCAS and ACM SIGCHI. DIAC-90 is partially supported by  
the National Science Foundation under Grant No. 8811437, Ethics and Values  
Studies Office.

The symposium will run from 9:00 am to 6:00 pm. Registration will start at  
8:15 am. Lunch will be provided. A reception will follow.

For additional information, contact symposium co-chairs: Coralee Whitcomb  
(617-891-3103 (weekdays), 508-945-0360 (weekends), or Peter Russo  
(206-965-1976, prusso@atc.boeing.com).

-----  
DIAC-90 Registration Form

Name:

Address:

Phone:

E-Mail:

Conference Fees:

CPSR Member     \$40 \_\_

Non-member     \$50 \_\_

Student         \$25 \_\_

Proceedings Only     \$20 \_\_

Please make checks payable to DIAC-90. Send registration to: DIAC-90, c/o  
CPSR/LA, P.O. Box 66038, Los Angeles, CA 90066-0038.



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 9: Issue 94

Friday 25 May 1990

## Contents

- [More on Stamford CT Telephone Switch Outage](#)  
[PGN](#)
- [Duplicate RISKS mailings...SOLVED!](#)  
[Emmett Hogan](#)
- [Cross about CRIS \(Crime Report information System\)](#)  
[Pete Mellor](#)
- [Disk failures after extended shutdown](#)  
[David Keppel](#)
- [The Internet is growing up!](#)  
[Scott Deerwester](#)
- [Are government secrets safer if not classified?](#)  
[Mary Culnan](#)
- [Risks of slandering ... in public forums \[re: P.T.U.U.I.\]](#)  
[Tom Blinn](#)
- [A320 again](#)  
[Nancy Leveson](#)
- [M1 Air Crash Inquest](#)  
[Brian Randell](#)
- [Tempus Fugit -- Claremont Clock Tower Tick Talk](#)  
[Brian Randell](#)
- [Telephone network synchronization and NavSat](#)  
[John T. Mulqueen via James Price Salsman via JC%RMC](#)
- [National Geographic also wants me to move](#)  
[Tim Kay](#)
- [Re: Irrational and nonvaledictory reasoning](#)  
[John Chew](#)
- [Info on RISKS \(comp.risks\)](#)

---

✉ **More on Stamford CT Telephone Switch Outage ([RISKS-9.93](#))**

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

Fri, 25 May 1990 14:37:39 PDT

AT&T announced today that they have resolved most of the cause of last

Thursday's 18-hour local-call switch outage. Apparently 10,000 subscribers were being moved from the #1A ESS to the new #5 ESS. During the cutover there is apparently a two minute atomic-action interval during which nothing works. Due to a burp, call storage was lost altogether. They found processor problems that have STILL not been diagnosed. They also found a cable that had been incorrectly connected last summer, and that remained undetected until the crash. When the backup failed as well, diagnostics could not be run except by old-fashioned oscilloscopic probes. [Source: Brief phone conversation with Seth Angott of The Advocate in Stamford CT. Any inaccuracies are mine.]

---

## ✂ Duplicate RISKS mailings...SOLVED!

Emmett Hogan <hogan@csl.sri.com>

Fri, 25 May 90 14:25:26 -0700

The nasty bug that was hitting the RISKS Digest mailings has been discovered and dealt with (hopefully, never to rear its ugly head again). Apparently, the problem did not lie with sendmail at all, but instead with a cron job that was running on our mailhost. The purpose of this job was to fix a very old bug in sendmail which would result in messages sitting in the mail queue forever.

The cron job worked like this:

- 1) Check to see what sendmail processes are running, Keep track of them.
- 2) If a sendmail process has been running since the last time through, kill it. It basically assumes that a queue should be processed in a certain amount of time (back to 6th grade..."you know what happens when you assume....")

Well, with the advent of nameservers, it is not abnormal for a message with a large number of recipients (i.e. RISKS Digest) to take quite a while to run. And because of the varying response time of the nameservers, a list which processed quickly one time might take a while longer the next...hence different RISKS sublists were hit each time. To add to the problems, this code was buried in a cron job which needs to be run to clean up the mail queue directory.

PLEASE NOTE: This does NOT fix the problems on BITNET, where people are receiving duplicate mailings. There is a group of people at Penn State who have dedicated their existence to solving this problem :-).

Jim Duncan (jim@augusta.math.psu.edu) explained what SEEMS to be the BITNET problem:

The problem is that there are multiple sites gatewaying certain mailing lists and newsgroups, and they don't do it in a consistent manner. Also, some of the problem is due to the differences in the plethora of news propagation packages (Bnews, Cnews, Netnews) out there on Usenet.

We're trying to solve the problem by initially setting up a registry for

BITNET<-->LISTSERV<-->Usenet gateways. We'll make sure there's only one site gating a certain group, and hopefully cut down on the problem significantly. When we get that under control, we're going to attack the other problems. But first we want to get a handle on the gateways.

By the way, the group of people looking after this project can be reached at <news-admin@cs.psu.edu>. If someone wants to know more, ask'em to send mail there.

Emmett Hogan            Computer Science Lab, SRI International  
UUCP: {ames, decwrl, pyramid, sun}!fernwood!hercules!hogan  
USMAIL: BN179, 333 Ravenswood Ave, Menlo Park, CA 94025  
ICBM: 37d 27' 14" North, 122d 10' 52" West

---

### **✂ Cross about CRIS (Crime Report information System)**

*Pete Mellor <pm@cs.city.ac.uk>  
Fri, 25 May 90 21:31:42 PDT*

>From the Guardian Computer section, Thursday, May 24:

Headline: "Police start to get cross about Cris"

"The Met [Metropolitan Police Force] is computerising its system of recording reported offences, but villains will be happy to hear that the scheme is behind schedule. Sid Smith reports:

A crime-busting computer network, which revolutionises police methods of storing records, is so late that the police are claiming compensation from the system designers [SD-Scicon]. And police staff say that such delays are typical of government tendering methods.

Cris, the &17 million Crime Report information System, will replace the archaic written crime books used at London police stations to record reported offences.

[stuff omitted]

Instead of entering crime reports into unmanageable written records, police staff will type the data into computer terminals at the police station. The data will then be passed to a DEC MicroVAX minicomputer at the local divisional headquarters, which in turn will copy it to duplicate database on a multi-node VAXcluster at the Metropolitan Police's central computer facility."

To summarise: The Met thinks this will be the largest relational database in Europe. Response times should generally be a few seconds. 2000 terminals in 200 buildings will handle 1 million crime reports a year. The purpose is to cross-search all other reports for any new crime reported. It should be particularly useful for "putting additional crimes for a prisoner to take into consideration".

The general non-criminal public will have access under the Data Protection Act.

The report goes on to say:

"The importance of public access to files was underlined earlier this year by a case in the Watford area. A clerk operating a computer at a local magistrates court entered the crime code 216 instead of 261. As a result, several individuals were accused of unlawful sexual intercourse instead of the correct alleged offence - using a TV set without a licence."

On the following page of the same issue of the Guardian is another article headed "The insidious growth of Gigo and how to halt it".

There we read that: "The most common form of clerical error is transposing digits (writing 1324 instead of 1234). Check-digits prevent transposition errors on coded information..."

One hopes that the designers of CRIS read the Guardian :-)

Peter Mellor, Centre for Software Reliability, City University, Northampton Square, London EC1V 0HB

---

### **✂ Disk failures after extended shutdown**

*David Keppel <pardo@cs.washington.edu>  
22 May 90 05:22:31 GMT*

Recently, a several-hour power failure shut down all of our computers. Most of the computers rebooted from this unexpected failure. Our largest VAX, however, refused to reboot. When DEC field service arrived, they were able to reboot the machine only by replacing several of the hard disks. The data that had been written since the last backup was completely lost.

Apparently, there have been problems with some of the RA90 disks. When they are shut down and restarted, they function normally. Apparently, however, if they are shut off long enough to cool down, the bearing seals fail and oil is spewed all over the disks. This failure has apparently been observed in a small but significant (a few percent) of the disks.

A point to ponder: The last I heard, DEC had not told its customers. The aware customer may be able to avoid extended shutdowns and/or do backups just before shutdown. Also, the aware customer may be able to plan an extended shutdown just before a planned field service call, allowing the user to explore possible failure in a planned way.

---

### **✂ The Internet is growing up!**

*Scott Deerwester <scott@sage@gargoyle.uchicago.edu>  
Fri, 25 May 90 10:45:57 CDT*

Consider:

5/8: Jim Vavrina reads Nick DiGionanni's description of Military

Viruses in VIRUS-L 3-90.

5/10: Jim gets a FAX of Rory O'Connor's article, and finds the person that Rory interviewed. Jim writes an article to the net, which David Brierly forwards on 5/13 to RISKS.

5/11: Andy Warinner gives a summary of an SBIR solicitation that is probably the source of Nick's description.

5/20: Rory O'Connor reads Jim's article on the net, and responds in RISKS to the charges that Jim made.

All of this happened in the space of a little over a week, all over the net. I don't find it remarkable when a bunch of computer types chat at each other over the net. But the fact that most of the people involved in this incident (and I have *\*no\** comment on the incident) can all chat about it over the net, including a reporter for a San Jose paper. Amazing.

Scott Deerwester, Center for Information and Language Studies, University of Chicago, 1100 E. 57th, CILS Chicago, IL 60637 Phone: 312-702-6948

---

### **✂ Are government secrets safer if not classified?**

*<mculnan@guvax.georgetown.edu>*

*22 May 90 07:55:00 EDT*

In his most recent newsletter, Senator Daniel Patrick Moynihan (D-NY) writes:

"Something called, I'm sorry to say, the Information Security Oversight Office located in the General Services Administration, has just reported that in 1989 the government created 6,796,501 new secrets. Half again the number of new babies. Is it not likely that the present system of classification actually calls attention to things we would closely hold? If an envelope is marked TOP SECRET -- one of the lower classifications by the way -- does that make a spy's work easier?"

There must be some amateur mathematicians and cryptographers who receive this newsletter. Would anyone care to demonstrate that real secrets-- I would judge there are maybe one hundred new ones every year -- would be safer if *\*NOT\** classified? I will insert selected replies in the Congressional Record. (Which incidentally is a good hiding place for secrets. Even the Russians are known to have despaired of deciphering it)."

Any ideas should be sent directly to Senator Daniel Patrick Moynihan, U.S. Senate, Washington, D.C. 20510.

Mary Culnan, School of Business Administration, Georgetown University

---

### **✂ Risks of slandering identifiable individuals/businesses in public forums**

*"Dr. Tom @MKO, CMG S/W Mktg, DTN 264-4865" <blinn@dr.enet.dec.com>*

*Tue, 22 May 90 07:16:02 PDT*

[RISKS DIGEST 9.93](#) (Monday 21 May 1990) included an announcement of P.T.U.U.I. from Robert Hardy (a195@mindlink.UUCP).

Since this appears to be a "bulletin board" and presumably allows unrestricted public access, anyone considering posting the sort of contributions that are being sought might want to also consider the risks of being taken to court on civil charges of slander, business defamation, and the like. Even though the BBS operator may be able to disclaim responsibility (through a "freedom of the press" argument, for instance), identifiable contributors probably can not get the same freedom. Of course, contributors can "fake" their names so that they can not be traced (unless it's one \*HELL\* of a clever BBS, in which case using one of the 1-900 route-through services would probably fool it), but how much credence can anyone place in \*anonymous\* slander?

Clearly, there are RISKS in working for small businesses, and especially in working for individuals. Most of those risks can be controlled by checking references (you \*can\* ask a prospective employer for references, after all), by making sure your own rights are spelled out in a contract between you and your employer, and so forth. In other words, there are better ways to make sure your own rights are protected than by participating in organized slander.

>We would like to act as an `Ombudsman' to mediate disputes.

Acting as an "Ombudsman" is very different from acting as a clearinghouse for unsubstantiated and perhaps inaccurate defamatory statements.

Tom

Dr. Thomas P. Blinn, Marketing Consultant, Application Platforms, U. S. Channels, Digital Equipment Corporation, Continental Blvd. -- MKO2-2/F10 Merrimack, New Hampshire 03054  
Usenet: ...!decwrl!dr.enet.dec.com!blinn Phone: (603) 884-4865

---

## **A320 again**

*Nancy Leveson <nancy@safety.ICS.UCI.EDU>  
Thu, 24 May 90 02:16:38 -0700*

The 21 May 90 issue of Newsweek has an article on the A320. It gibes with the rumors I have heard from people in the aircraft industry (although they have told me about even more suspected control systems problems than are mentioned in this article).

A Bumpy Ride for the Airbus A320:  
Northwest's newest fleet comes under scrutiny  
by Annetta Miller with Karen Springen

"It's been one of the more controversial aeronatic introductions since Kitty Hawk. And last week the highly automated Airbus A320 jetliner bumped up against still more turbulence. Northwest Airlines, the only U.S. carrier to operate the planes, acknowledged that it has reported suspected malfunctions of the aircraft's flight control system to the Federal Aviation Administration.

The reports come on the heels of two overseas crashes involving the \$32 million plane. While both Northwest and the plane's manufacturer say it is safe to fly, the crashes and the reports to the FAA raise questions about its reliability -- and the limits of technology. 'The controversy is always out there,' says Edwin Arbon of the Flight Safety Foundation. 'Are we going too far with automation?'"

---

## ✈ M1 Air Crash Inquest

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

Wed, 23 May 90 16:37:20 BST

Today's UK newspapers carry lengthy accounts of the results of the inquest that has just been held into the deaths arising from the Kegworth (M1) air crash. Here, quoted without permission, are two articles from the Independent. About half of the first article is included, and all the second. (Other articles have the titles "Decision by pilots to switch off good engine remains a mystery" and "Training of cabin crew may change".)

Brian Randell

:: "Lessons must be learnt from M1 air crash, inquest told."  
:: - by Stephen Ward  
::  
:: The coroner at the inquest into the deaths of 47 people in the M1 air  
:: crash yesterday listed eight areas where he believed safety could be  
:: improved.  
:: .....  
::  
:: The crash happened after one of the aircraft's engines malfunctioned  
:: but the pilots switched off the wrong one. Mr Tomlinson said he would  
:: be writing to the Department of Transport's Air Accident Investigation  
:: Branch (AAIB) and to the Civil Aviation Authority regulatory body with  
:: a list of areas he thought were important.  
::  
:: -The relationship between the cockpit crew and the cabin crew,  
:: particularly in an emergency. (The cabin staff saw fire from the  
:: left-hand engine, but did not tell the pilots.)  
::  
:: - Urgent provision of external cameras and monitor screens so pilots  
:: can see the outside of the aircraft, including the engines.  
::  
:: - Warning lights on the vibration monitor instruments, as  
:: 'attention-getters' and to identify which engine was at fault.  
::  
:: - Red areas on the vibration dials when they approach danger levels,  
:: as with other instruments.  
::  
:: - New or modified types of engines to be tested in flying conditions  
:: before approval. (The CFM-56 engine in the crash had only been  
:: bench-tested).  
::

:: - Pilot training to emphasise the importance of new instrument  
:: systems, particularly where they replace an instrument which has been  
:: largely ignored in the past. (Early vibration monitors were  
:: unreliable).

::  
:: - Design of instrument panels, and their relationship with other  
:: controls. (The 737-400 had new, electronic dials).

::  
:: - The factors in the design of the cabin which meant some passengers  
:: survived the impact while others died.

:: .....

:: -----

:: "High-tech cockpits `may be gap in safety' "

:: - by David Black, Transport Correspondent

::  
:: `Glass cockpits' like the one on board the British Midland Boeing 737  
:: that crashed at Kegworth, are of a design close to the cutting edge of  
:: aviation technology. The decision to introduce them was a matter of  
:: economics.

::  
:: Everyone should have been happy - the airline because it was going to  
:: cost them less to fly 'glass cockpit' jets, which incorporate six  
:: cathode ray tubes in place of the electro-mechanical guages in older  
:: airlines; passengers because tickets would be cheaper; and pilots  
:: because the new gadget would cut workload.

::  
:: However, the recent spate of seemingly inexplicable accidents and  
:: incidents involving these new high-tech airliners points to a gap in  
:: aviation's safety defences. In their pursuit of efficiency, the  
:: industry may have brought the environment of pilots into the age of  
:: information but omitted to teach them how to manage it.

::  
:: The Kegworth inquest is over but the official report by the Department  
:: of Transport's Air Accidents Investigations Branch has yet to come.

::  
:: Although written, it is unlikely to be published before late summer.  
:: But it is understood that it is not the flight deck crew, who  
:: mistakenly shut down the wrong engine, that come in for most  
:: criticism, but the design of the 737' `glass cockpit' and the training  
:: that crew receive in operating it.

::  
:: The computer systems that run the `glass cockpits' are also subject  
:: to question after two crashes of the world's most advanced  
:: computerised airliner, the Airbus A320, and other incidents in which  
:: the computer overrode the crew's commands and `crashed' the aircraft,  
:: despite efforts to prevent it.

::  
:: Behind these problems lies the deceptive simplicity of `glass cockpit'  
:: operations. In an old cockpit, there are several hundred guages  
:: feeding off many more sensors, the guages maintained with all the  
:: skills of a watchmaker.

::  
:: However, in a `glass cockpit' there are only the six cathode ray

:: tubes, as in an ordinary television, and if one fails the information  
:: displayed on it can be punched up on its neighbour. Repair is  
:: achieved by unplugging the component and plugging in another.  
::  
:: The system works because all the sensors feed their information into  
:: three flight management computers, each policing the the other for  
:: mistakes. They take responsibility for the information the pilot sees  
:: on his screen. The pilot's workload is cut because the computer will  
:: assess each problem for him.  
::  
:: The computers will also identify the nature of the fault and present  
:: the pilot with a checklist of action to be taken.  
::  
:: Herein lies the deception. While six screens have replaced up to 400  
:: instruments, the information passing through those screens is vast.  
:: In one column alone on a flight management display, different messages  
:: the equivalent of three A4 pages in length can flash up, and each of  
:: those can be colour-coded to represent a different status. The pilot,  
:: to understand what his aircraft is doing, must first understand what  
:: the computer is doing.  
::  
:: That flies in the face of basic airmanship and pilots' comments  
:: reflect the dilemma. One said: "With old cockpits the workload was  
:: high but you were always aware of what's going on. Things either  
:: worked or they didn't. With the computer you have to back-track to  
:: find the initial error before you can correct "  
::  
:: Another commented: "With a flight management computer there is almost  
:: a sense of disbelief. You ask "Why's it doing that?" and then you get  
:: sucked into an intellectual exercise of trying to work out what is  
:: going on."  
::  
:: "Why is it doing that?" is the most common phrase passing between  
:: pilot and co-pilot on a modern jet, according to Dr Roger Green, of  
:: the RAF's Institute of Aviation Medicine. In a lecture to the Royal  
:: Aeronautical Society he said: "Modern pilot training methods [and  
:: `glass cockpits'] are distancing the pilot from his aircraft and  
:: environment."  
::  
:: When the unexpected happened, the pilot was less likely to be able to  
:: deal with the emergency quickly or accurately, he said.  
::  
:: Pilots feel that the transfer of computer technology from office to  
:: cockpit has gone through on the nod without anyone paying attention to  
:: the different working environments. If this quantum leap in aviation  
:: technology is to succeed, more attention must be paid to the human  
:: factor.  
::  
:: Captain Kevin Hunt, the pilot in the M1 crash, was very experienced  
:: but had flown the 737 type that crashed for only 23 hours. His  
:: co-pilot had only 53 hours on the type. Each had received only a  
:: day's classroom training on its instruments, the inquest was told.  
::

:: The AAIB report's likely recommendations on cockpit design and pilot  
:: training seem to indicate that they, too, are coming to share the  
:: pilot's worries

---

## ✂ Tempus Fugit

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

Fri, 25 May 90 13:08:41 BST

[RISKS 9.32](#) carried a message from me about the master/slave clock system in the Claremont tower at the University of Newcastle upon Tyne. (The gist of the message was that the design was totally - indeed unbelievably - inadequate, through failing to provide \*any\* means of synchronising the slave clocks from the master, e.g for fault tolerance purposes, or for summer time changes.)

I thought RISKS readers might be amused by how this 25-year old system has suddenly come to the end of the line.

Recently workmen were found in the Tower, tiling a patch of wall, on each level, to make good damage caused by installation and refurbishment of the lift (elevator) systems. Quite aside from the fact that the result of such ("lavatory") tiling was aesthetically unpleasing, to say the least, we complained at the lost opportunity. By this I mean that the tiler was carefully, and with great difficulty, cutting large circular holes in the tiles, to allow the slave clocks to be re-installed in the walls!

A colleague edited the ensuing email correspondence within the Computing Lab about this activity, plus my original RISKS posting, to produce a document to accompany a request to our Bursar's Office that this work be halted and the clock system be removed instead. This request was answered far faster than past experience with this Office would have led us to expect - indeed almost immediately after the tiling was complete!

Moreover the answer was much more positive than we expected - the clock system was to be removed, and the holes in the tiling made good. In fact this work started on the very day that the reply arrived. So the offending system is now no more, though there is a strong possibility that the rather fine looking master clock will be put on display somewhere in the Computing Laboratory (with an account of how RISKS helped in its demise). However if anybody wants a large number of slave clocks, our Bursar's Department might be able to help them!

Brian Randell, Computing Laboratory, University of Newcastle upon Tyne, UK  
PHONE = +44 91 222 7923 FAX = +44 91 222 8232

---

## ✂ Telephone network synchronization and NavSat

<JC%RMC@ugw.utoronto.ca>

Wed, 23 May 90 01:26:55 EDT

The following is excerpted from SPACE Digest V11 #419. The phone companies seem to have assumed that DoD would not change the operation of their

NavStar satellites. This sounds to me like another example of using a non-standard 'feature' and being stung for it later.

Date: Thu, 17 May 90 18:07:06 -0400 (EDT)  
From: James Price Salsman <js7a+@andrew.cmu.edu>  
Subject: GPS/NAVSTAR news

>From \_Data\_Communications\_ (ISSN 0363-6399) vol. 19, no. 6, May 1990, p. 56  
(c) 1990 McGraw-Hill Inc

#### DOD DITHERS DIGITAL DATA

Telephone network synchronization is an unlikely topic for heated controversy, but that is what the U.S. Department of Defense has provoked by tampering with the Navstar Global Positioning Satellite (GPS) system that AT&T plans to use as a network clock.

GPS is a group of 13 satellites now in operation and 27 more to be launched by 1994 [I believe this is in error, as there are to be 27 total satellites in the constellation --jps], each of which produces and encrypted P code that the military uses to guide missiles, and another signal, called the Clear/Acquisition signal, that has been available for commercial uses like surveying and timing communications networks.

But the DoD has decided that even the C/A signal is too accurate to be generally available, so it has begun a practice it calls "selective availability." That delicious piece of bureaucratese means that the DoD will introduce random noise on the C/A signal, known in some circles as "dithering," to make it difficult or even impossible to use.

Meanwhile, some commercial equipment manufacturers and users, such as land surveyors, are already relying on the signal and now are angry that the DoD is changing the rules. "There is a big controversy about why the government is doing this," says Jim Jespersen, a staff member of the time and frequency division of the National Institute of Standards and Technology (Boulder, Colo.), "especially since the threat from the Russians is not so severe." [The "Russians" have a very accurate GPS system of their own, called GLONASS, so someone is confused here... --jps]

GPS is run by the U.S. Air Force Systems Command's Space Division in Los Angeles. The officer in charge of the project, Col. Marty Runkle of the Joint Program Office, could not be reached for comment.

As for AT&T, George Zampetti, a Bell Laboratories scientist who is in charge of developing AT&T's synchronization scheme, says that the company plans to use the C/A signal even if it is dithered.

Zampetti and John Abate, another Bell Labs scientist, say AT&T will use 3B2 computers to filter out the noise to get close to the true signal. Filtering will slow down but not eliminate the use of GPS, Abate says.

"We could go a month and still maintain" on error in 100 billion events, Zampetti says.

The key to the system is Rubidium clocks that actually pass timing to AT&T's switches and transmission network. Those Rubidium clocks can maintain network timing to meet requirements of ANSI and CCITT standards, Zampetti says. AT&T would use GPS to calibrate and monitor the rubidium clocks. -John T. Mulqueen

[The main article (of which that was a sidebar) talks about MCI and Sprint's use of Loran, atomic clocks, and describes GPS. The ANSI standard in question is T1.101, by committee T1X1.3, which describes synchronization for high-bandwidth long-haul digital transmission. --jps]

---

### **✂ National Geographic also wants me to move ([RISKS-9.73](#))**

<tim@ggumby.cs.caltech.edu>

Tue, 22 May 90 13:34:08 PDT

I reported earlier that United MileagePlus couldn't get my address straight. I told them Timothy L. Kay, Box 256-80, Pasadena, CA 91125 and they kept changing my zip code to 91102. Then I started seeing this problem with several other companies, all from the eastern half of the United states. I have asked them for help in debugging the problem, and they all point their fingers at the US Postal Service, but none of them has yet given me a name to talk to.

National Geographic has graciously sent me every issue by first class mail as soon as I report that it is late. The postage comes to about \$2.25 per issue. That is pretty generous of them, considering that my subscription for 12 monthly issues is \$21.00. That is the price they pay if they can't tell their computer to ignore (erroneous) redirects from the Post Office.

My favorite memorabilia (so far) is a letter from National Geographic that says that the Post Office has told them that this address is no good, and could I please inform them of a good one. Of course, they sent the letter to the "bad" address. It reminds me of an IBM PC clone that booted with the following error message:

"... missing keyboard; hit F1 to continue."

---

### **✂ Re: Irrational and nonvaledictory reasoning**

John Chew <john@trigraph.uucp>

Wed, 23 May 90 17:11:10 EDT

In [RISKS DIGEST 9.93](#), "Peter G. Neumann" <neumann@csl.sri.com> quoted a UPI report that three Florida seniors had obtained GPAs of 4.2857142, and then suggested "that no one along the way recognized 4 and two sevenths in disguise."

Well, if \*my\* GPA were actually 30/7 and a school had salami'd me of almost an entire unit in the last digit of the calculated figure (the correct value of 4.285714 2857142 ... is of course \*much\* closer to 4.2857143), I'd be posting now to complain about the risks of grade-point truncation. :-)

[A Bit Off More Than You Could Chew? 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 9: Issue 95

Saturday 26 May 1990

## Contents

- [Possible Anti-Virus Legislation](#)  
[Robert Smithmidford](#) via [Thomas Zmudzinski](#) via [Linda K. Perez](#)
- [Secure UNIX Infected?](#)  
[Craig Harmer](#) via [Russ Davis](#) via [Linda K. Perez](#)
- [Follow-up on Fed Raids on Hackers](#)  
[David Ruderman](#)
- [Crypto '90 conference, 11-15 August 1990, UC Santa Barbara](#)  
[John Gilmore](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✂ Possible Anti-Virus Legislation

*Linda K. Perez <lkperez@nasamail.nasa.gov>*  
*22 May 90 13:51:00 GMT*

Forwarded message: [via indirect routing]  
Date: 16 May 90 10:44:00 -0400  
From: "zmudzinski, thomas" <zmudzinskit@imo-uvax.dca.mil>  
Subject: Possible Anti-Virus Legislation

>From Federal Computer Week, 14 May 90, P.14 & 17      -- QUOTE --

Congress Expected to Pursue Stricter Computer Virus Laws

By ROBERT SMITHMIDFORD

In the wake of Robert Morris Jr.'s conviction for unleashing the Internet worm in 1988, both the House and Senate are expected to take up bills that would make computer viruses and other intentional sabotage specifically illegal.

Sen. Patrick Leahy (D-Vt.) recently introduced the latest virus bill, S2476. The bill would make it a federal felony to gain access to computers intentionally and to introduce destructive programs that cause a

\$1,000 loss over the course of a year. Sabotage that effects medical records would also be illegal. The bill also would allow people who suffer losses from a virus or other malicious program to file civil suits to get compensation.

According to Ron Palenski, general counsel for the trade association Adapso, Leahy's bill is stronger than pending legislation in the House because it expands what might be considered a virus. "The strength of the Leahy proposal is that it takes an interstate commerce approach. Since virtually anything is in interstate commerce, it covers almost anything," Palenski said. Current law covers only computers owned by the government or a financial institution or cases in which viruses are spread across state lines, he said. Leahy's bill also adds viruses embedded in software to its definition of gaining access to computers. "The current statute is really written in terms of networks. It assumes that the vandalism will occur in networks, but it can also occur in distributed software," Palenski said.

However, the bill might be open to modification. In proposing the bill, Leahy said, "I want to ensure that in creating a private cause of action to boost deterrence we do not open the floodgates to frivolous litigation. I also look forward to testimony from prosecutors and computer experts on the scope of the access definition, to be sure that it is technically sound and a useful tool from prosecuting computer crimes."

The Computer and Business Equipment Manufacturers Association applauded the legislation for focusing on criminal behavior by individuals, not by restricting technology.

"It's completely proper that we make it clear that what we thought of as a prank isn't a game anymore," said Jude Franklin, a senior vice president for technology at Planning Research Corp. But finding the source of viruses can be difficult. "There are going to be problems enforcing it because third parties aren't aware they're carrying them," he said.

Hearings are expected in June.

The Morris sentencing also is likely to dislodge two similar bills awaiting action on the House side. HR 55 and 287, sponsored by Rep. Wally Herger (R-Calif.) and Rep Tom McMillen (D-Md.) respectively, were on hold in the House Judiciary Committee pending comments from Justice.

-- UNQUOTE --



LINDA K. PEREZ <lkperez@nasamail.nasa.gov>  
22 May 90 14:05:00 GMT

Forwarded message:

Posted: Fri, May 18, 1990 8:49 AM PDT      Msg: SJJJ-2884-8051  
From: RDAVIS

Subj: Secure UNIX Infected?

If you read between the lines you will note that a development version of AT&T UNIX was infected. The message is that the "NCSC" is more concerned about "confidentiality" then, say, integrity. The sooner we get a counter balance to the NCSC critical mass within POSIX P1003.6 (security) the better our future.

Russ

Date: Fri, 18 May 90 01:42:02 +0000

From: craig@tolerant.com (Craig Harmer)

Subject: Re: mainframe viruses should be as complex as pc viruses

teda!RATVAX.DNET!ROBERTS@decwrl.dec.com (George Roberts) writes:

>Jim Molini explained how it is difficult to infect an MVS system. I

>don't even know what computer MVS runs on (IBM?), let alone details

>about the operating system.

>

>Let me say (in my opinion) that in VAX/VMS, it is no easier and no

>harder to write an executable infecting virus than it is in MSDOS.

>

>The virus is written basically the same way as it would be for a pc. Here

>are some of the steps:

>1) Search for files with extension \*.exe.

>2) Check if already infected.

>3) Read the file-to-infect and create a new file with the same name,

> but one version higher.

>4) Change the execution transfer address to near the end of the file

> (or change the first instruction to a jmp to the end of the file).

>4) Add the virus code at the end of the file.

>5) Add a jump at the end of the virus to the begining of the .exe file.

#...

>- George Roberts

>.decwrl.dec.com!teda!ratvax.dnet!roberts

it's been done. at the Winter '89 Usenix conference in san diego, Tom Duff presented a paper entitled "Viral Attacks on UNIX System Security". he built a virus somewhat weaker than the one described above; it would only insert itself in the extra space at the end of an executable, if there was sufficient space between the end of the executable and the next 512 byte block boundary. if would only infect files in the current directory.

he loosed the thing inside AT&T as an experiment to see how well such a weak virus would spread, and how it could be started. (he started the infection by adding an infected copy of "echo" to some public directories he had write access too).

the most interesting aspect of this was that it got picked up in an automated distribution of a new version of "wc" to 45 local machines, at which time the infection really took off. it caused some particular problems on a "secure" unix that was being developed, since the kernel detected the attempts of the virus to propagate, and killed the virus. unfortunately, it had by then gotten imbedded in cc, as, and all the other important utilites as a result of "big make" performed with the security checks turned off.

it's an interesting paper; one worth reading, since it talks about means of prevention, and generally good security practice on Unix machines.

{apple,pyramid}!tolsoft!craig      craig@hoser.tolerant.com  
(415) 626-6827 (h)                    (408) 433-5588 x220 (w)  
[views expressed above shouldn't be taken as Tolerant's views, etc. ...]

---

## ✂ Follow-up on Fed Raids on Hackers (Including factual information)

David Ruderman <ruderman@sbc.suny.edu>  
Tue, 22 May 90 14:49:22 EDT

THE FOLLOWING TWO ARTICLES ARE FROM THE JUST-RELEASED SPRING EDITION OF 2600 MAGAZINE, THE HACKER QUARTERLY. WE FEEL THAT THE CURRENT HAPPENINGS IN THE COMPUTER WORLD ARE EXTREMELY SIGNIFICANT FOR ANYONE WHO HAS ANY INTEREST IN COMMUNICATIONS AND/OR TECHNOLOGY. WE'D BE MOST INTERESTED IN ANY FEEDBACK ON THIS TOPIC. [See the end of this message.]

\*\*\*\*\*  
ARTICLE ONE: AN OVERVIEW  
\*\*\*\*\*

A year ago, we told the stories of Kevin Mitnick and Herbert Zinn, two hackers who had been sent to prison. It was then, and still is today, a very disturbing chain of events: mischief makers and explorers imprisoned for playing with the wrong toys and for asking too many questions. We said at the time that it was important for all hackers to stand up to such gross injustices. After all, they couldn't lock us all up.

It now appears that such an endeavor may indeed be on the agendas of some very powerful U.S. governmental agencies. And even more frightening is the realization that these agencies don't particularly care who or what gets swept up along with the hackers, as long as all of the hackers get swept up. Apparently, we're considered even more of a threat than we had previously supposed.

In retrospect, this doesn't come as a great deal of a surprise. In fact, it now seems to make all too much sense. You no longer have to be paranoid or of a particular political mindset to point to the many parallels that we've all been witnesses to. Censorship, clampdowns, "voluntary" urine tests, lie detectors, handwriting analysis, surveillance cameras, exaggerated crises that invariably lead to curtailed freedoms.... All of this together with the overall view that if you're innocent, you've got nothing to hide. And all made so much more effective through the magic of high tech. Who would you target as the biggest potential roadblock if not the people who understand the technology at work? It appears the biggest threats to the system are those capable of manipulating it.

What we're about to tell you is frightening, plain and simple. You don't have to be a hacker to understand this. The words and ideas are easily translatable to any time and any culture.

Crackdown

"We can now expect a crackdown...I just hope that I can pull through this one and that my friends can also. This is the time to watch yourself. No matter what you are into.... Apparently the government has seen the last straw in their point of view.... I think they are going after all the 'teachers'...and so that is where their energies will be put: to stop all hackers, and stop people before they can become threats."

This was one of the reactions on a computer bulletin board to a series of raids on hackers, raids that had started in 1989 and spread rapidly into early 1990. Atlanta, St. Louis, and New York were major targets in what was then an undetermined investigation.

This in itself wouldn't have been especially alarming, since raids on hackers can almost be defined as commonplace. But this one was different. For the very first time, a hacker newsletter had also been shut down.

Phrack was an electronic newsletter published out of St. Louis and distributed worldwide. It dealt with hacker and phone phreak matters and could be found on nearly all hacker bulletin boards. While dealing with sensitive material, the editors were very careful not to publish anything illegal (credit card numbers, passwords, Sprint codes, etc.). We described "Phrack World News" (a regular column of Phrack) in our Summer 1989 edition as "a must-read for many hackers". In many ways Phrack resembled 2600, with the exception of being sent via electronic mail instead of U.S. Mail. That distinction would prove to be Phrack's undoing.

It now turns out that all incoming and outgoing electronic mail used by Phrack was being monitored by the authorities. Every piece of mail going in and every piece of mail coming out. These were not pirated mailboxes that were being used by a couple of hackers. These had been obtained legally through the school the two Phrack editors were attending. Privacy on such mailboxes, though not guaranteed, could always be assumed. Never again.

It's fairly obvious that none of this would have happened, none of this could have happened had Phrack been a non-electronic magazine. A printed magazine would not be intimidated into giving up its mailing list as Phrack was. Had a printed magazine been shut down in this fashion after having all of their mail opened and read, even the most thick-headed sensationalist media types would have caught on: hey, isn't that a violation of the First Amendment?

Those media people who understood what was happening and saw the implications were very quickly drowned out in the hysteria that followed. Indictments were being handed out. Publisher/editor Craig Neidorf, known in the hacker world as Knight Lightning, was hit with a seven count indictment accusing him of participating in a scheme to steal information about the enhanced 911 system run by Bell South. Quickly, headlines screamed that hackers had broken into the 911 system and were interfering with emergency telephone calls to the police. One newspaper report said there were no indications that anyone had died or been injured as a result of the intrusions. What a relief. Too bad it wasn't true.

In actuality there have been very grievous injuries suffered as a result of these intrusions. The intrusions we're referring to are those of the

government and the media. The injuries have been suffered by the defendants who will have great difficulty resuming normal lives even if all of this is forgotten tomorrow.

And if it's not forgotten, Craig Neidorf could go to jail for more than 30 years and be fined \$122,000. And for what? Let's look at the indictment:

"It was... part of the scheme that defendant Neidorf, utilizing a computer at the University of Missouri in Columbia, Missouri would and did receive a copy of the stolen E911 text file from defendant [Robert J.] Riggs [located in Atlanta and known in the hacker world as Prophet] through the Lockport [Illinois] computer bulletin board system through the use of an interstate computer data network.

"It was further part of the scheme that defendant Neidorf would and did edit and retype the E911 Practice text file at the request of the defendant Riggs in order to conceal the source of the E911 Practice text file and to prepare it for publication in a computer hacker newsletter.

"It was further part of the scheme that defendant Neidorf would and did transfer the stolen E911 Practice text file through the use of an interstate computer bulletin board system used by defendant Riggs in Lockport, Illinois.

"It was further part of the scheme that the defendants Riggs and Neidorf would publish information to other computer hackers which could be used to gain unauthorized access to emergency 911 computer systems in the United States and thereby disrupt or halt 911 service in portions of the United States."

Basically, Neidorf is being charged with receiving a stolen document. There is nothing anywhere in the indictment that even suggests he entered any computer illegally. So his crimes are receiving, editing, and transmitting.

Now what is contained in this document? Information about how to gain unauthorized access to, disrupt, or halt 911 service? Hardly. The document (erroneously referred to as "911 software" by the media which caused all kinds of misunderstandings) is quoted in Phrack Volume 2, Number 24 and makes for one of the dullest articles ever to appear in the newsletter. According to the indictment, the value of this 20k document is \$79,449. [See story that follows this one]

Shortly after the indictments were handed down, a member of the Legion of Doom known as Erik Bloodaxe issued a public statement. "[A group of three hackers] ended up pulling files off [a Southern Bell system] for them to look at. This is usually standard procedure: you get on a system, look around for interesting text, buffer it, and maybe print it out for posterity. No member of LOD has ever (to my knowledge) broken into another system and used any information gained from it for personal gain of any kind...with the exception of maybe a big boost in his reputation around the underground. [A hacker] took the documentation to the system and wrote a file about it. There are actually two files, one is an overview, the other is a glossary. The information is hardly something anyone could possibly gain anything from except knowledge about how a certain aspect of the telephone company works."

He went on to say that Neidorf would have had no way of knowing whether or not

the file contained proprietary information.

Prosecutors refused to say how hackers could benefit from the information, nor would they cite a motive or reveal any actual damage. In addition, it's widely speculated that much of this information is readily available as reference material.

In all of the indictments, the Legion of Doom is defined as "a closely knit group of computer hackers involved in: a) disrupting telecommunications by entering computerized telephone switches and changing the routing on the circuits of the computerized switches; b) stealing proprietary computer source code and information from companies and individuals that owned the code and information; c) stealing and modifying credit information on individuals maintained in credit bureau computers; d) fraudulently obtaining money and property from companies by altering the computerized information used by the companies; e) disseminating information with respect to their methods of attacking computers to other computer hackers in an effort to avoid the focus of law enforcement agencies and telecommunication security experts."

Ironically, since the Legion of Doom isn't a closely knit group, it's unlikely that anyone will be able to defend the group's name against these charges -- any defendants will naturally be preoccupied with their own defenses. (Incidentally, Neidorf was not a part of the Legion of Doom, nor was Phrack a publication of LOD, as has been reported.)

#### The Hunt Intensifies

After learning of the Phrack electronic mail surveillance, one of the system operators of The Phoenix Project, a computer bulletin board in Austin, Texas, decided to take action to protect the privacy of his users. "I will be adding a secure encryption routine into the e-mail in the next 2 weeks - I haven't decided exactly how to implement it, but it'll let two people exchange mail encrypted by a password only known to the two of them.... Anyway, I do not think I am due to be busted...I don't do anything but run a board. Still, there is that possibility. I assume that my lines are all tapped until proven otherwise. There is some question to the wisdom of leaving the board up at all, but I have personally phoned several government investigators and invited them to join us here on the board. If I begin to feel that the board is putting me in any kind of danger, I'll pull it down with no notice - I hope everyone understands. It looks like it's sweeps-time again for the feds. Let's hope all of us are still around in 6 months to talk about it."

The new security was never implemented. The Phoenix Project was seized within days.

And the clampdown intensified still further. On March 1, the offices of Steve Jackson Games, a publishing company in Austin, were raided by the Secret Service. According to the Associated Press, the home of the managing editor was also searched. The police and Secret Service seized books, manuals, computers, technical equipment, and other documents. Agents also seized the final draft of a science fiction game written by the company. According to the Austin American-Statesman, the authorities were trying to determine whether the game was being used as a handbook for computer crime.

Callers to the Illuminati bulletin board (run by Steve Jackson Games), received the following message:

"Before the start of work on March 1, Steve Jackson Games was visited by agents of the United States Secret Service. They searched the building thoroughly, tore open several boxes in the warehouse, broke a few locks, and damaged a couple of filing cabinets (which we would gladly have let them examine, had they let us into the building), answered the phone discourteously at best, and confiscated some computer equipment, including the computer that the BBS was running on at the time.

"So far we have not received a clear explanation of what the Secret Service was looking for, what they expected to find, or much of anything else. We are fairly certain that Steve Jackson Games is not the target of whatever investigation is being conducted; in any case, we have done nothing illegal and have nothing whatsoever to hide. However, the equipment that was seized is apparently considered to be evidence in whatever they're investigating, so we aren't likely to get it back any time soon. It could be a month, it could be never.

"To minimize the possibility that this system will be confiscated as well, we have set it up to display this bulletin, and that's all. There is no message base at present. We apologize for the inconvenience, and we wish we dared do more than this."

Apparently, one of the system operators of The Phoenix Project was also affiliated with Steve Jackson Games. And that was all the authorities needed.

Raids continued throughout the country with reports of more than a dozen bulletin boards being shut down. In Atlanta, the papers reported that three local LOD hackers faced 40 years in prison and a \$2 million fine.

Another statement from a Legion of Doom member (The Mentor, also a system operator of The Phoenix Project) attempted to explain the situation:

"LOD was formed to bring together the best minds from the computer underground - not to do any damage or for personal profit, but to share experiences and discuss computing. The group has always maintained the highest ethical standards.... On many occasions, we have acted to prevent abuse of systems.... I have known the people involved in this 911 case for many years, and there was absolutely no intent to interfere with or molest the 911 system in any manner. While we have occasionally entered a computer that we weren't supposed to be in, it is grounds for expulsion from the group and social ostracism to do any damage to a system or to attempt to commit fraud for personal profit.

"The biggest crime that has been committed is that of curiosity.... We have been instrumental in closing many security holes in the past, and had hoped to continue to do so in the future. The list of computer security people who count us as allies is long, but must remain anonymous. If any of them choose to identify themselves, we would appreciate the support."

And The Plot Thickens

Meanwhile, in Lockport, Illinois, a strange tale was unfolding. The public UNIX system known as Jolnet that had been used to transmit the 911 files had also been seized. What's particularly odd here is that, according to the electronic newsletter Telecom Digest, the system operator, Rich Andrews, had been cooperating with federal authorities for over a year. Andrews found the files on his system nearly two years ago, forwarded them to AT&T, and was subsequently contacted by the authorities. He cooperated fully. Why, then, was his system seized as well? Andrews claimed it was all part of the investigation, but added, "One way to get [hackers] is by shutting down the sites they use to distribute stuff."

The Jolnet raid caused outrage in the bulletin board world, particularly among administrators and users of public UNIX systems.

Cliff Figallo, system administrator for The Well, a public UNIX system in California, voiced his concern. "The assumption that federal agents can seize a system owner's equipment as evidence in spite of the owner's lack of proven involvement in the alleged illegal activities (and regardless of the possibility that the system is part of the owner's livelihood) is scary to me and should be to anyone responsible for running a system such as this."

Here is a sampling of some of the comments seen around the country after the Jolnet seizure:

"As administrator for Zygote, should I start reading my users' mail to make sure they aren't saying anything naughty? Should I snoop through all the files to make sure everyone is being good? This whole affair is rather chilling."

"From what I have noted with respect to Jolnet, there was a serious crime committed there -- by the [federal authorities]. If they busted a system with email on it, the Electronic Communication Privacy Act comes into play. Everyone who had email dated less than 180 days old on the system is entitled to sue each of the people involved in the seizure for at least \$1,000 plus legal fees and court costs. Unless, of course, the [authorities] did it by the book, and got warrants to interfere with the email of all who had accounts on the systems. If they did, there are strict limits on how long they have to inform the users."

"Intimidation, threats, disruption of work and school, 'hit lists', and serious legal charges are all part of the tactics being used in this 'witch-hunt'. That ought to indicate that perhaps the use of pseudonyms wasn't such a bad idea after all."

"There are civil rights and civil liberties issues here that have yet to be addressed. And they probably won't even be raised so long as everyone acts on the assumption that all hackers are criminals and vandals and need to be squashed, at whatever cost...."

"I am disturbed, on principle, at the conduct of at least some of the federal investigations now going on. I know several people who've taken their systems out of public access just because they can't risk the seizure of their equipment (as evidence or for any other reason). If you're a Usenet site, you may receive megabytes of new data every day, but you have no common carrier protection in the event that someone puts illegal information onto the Net and

thence into your system."

#### Increased Restrictions

But despite the outpourings of concern for what had happened, many system administrators and bulletin board operators felt compelled to tighten the control of their systems and to make free speech a little more difficult, for their own protection.

Bill Kuykendall, system administrator for The Point, a public UNIX system in Chicago, made the following announcement to the users of his system:

"Today, there is no law or precedent which affords me... the same legal rights that other common carriers have against prosecution should some other party (you) use my property (The Point) for illegal activities. That worries me....

"I fully intend to explore the legal questions raised here. In my opinion, the rights to free assembly and free speech would be threatened if the owners of public meeting places were charged with the responsibility of policing all conversations held in the hallways and lavatories of their facilities for references to illegal activities.

"Under such laws, all privately owned meeting places would be forced out of existence, and the right to meet and speak freely would vanish with them. The common sense of this reasoning has not yet been applied to electronic meeting places by the legislature. This issue must be forced, or electronic bulletin boards will cease to exist.

"In the meantime, I intend to continue to operate The Point with as little risk to myself as possible. Therefore, I am implementing a few new policies:

"No user will be allowed to post any message, public or private, until his name and address has been adequately verified. Most users in the metropolitan Chicago area have already been validated through the telephone number directory service provided by Illinois Bell. Those of you who received validation notices stating that your information had not been checked due to a lack of time on my part will now have to wait until I get time before being allowed to post.

"Out of state addresses cannot be validated in the manner above.... The short term solution for users outside the Chicago area is to find a system closer to home than The Point.

"Some of the planned enhancements to The Point are simply not going to happen until the legal issues are resolved. There will be no shell access and no file upload/download facility for now.

"My apologies to all who feel inconvenienced by these policies, but under the circumstances, I think your complaints would be most effective if made to your state and federal legislators. Please do so!"

These restrictions were echoed on other large systems, while a number of smaller hacker bulletin boards disappeared altogether. We've been told by some

in the hacker world that this is only a phase, that the hacker boards will be back and that users will once again be able to speak without having their words and identities "registered". But there's also a nagging suspicion, the feeling that something is very different now. A publication has been shut down. Hundreds, if not thousands, of names have been seized from mailing lists and will, no doubt, be investigated. The facts in the 911 story have been twisted and misrepresented beyond recognition, thanks to ignorance and sensationalism. People and organizations that have had contact with any of the suspects are open to investigation themselves. And, around the country, computer operators and users are becoming more paranoid and less willing to allow free speech. In the face of all of this, the belief that democracy will triumph in the end seems hopelessly naive. Yet, it's something we dare not stop believing in. Mere faith in the system, however, is not enough.

We hope that someday we'll be able to laugh at the absurdities of today. But, for now, let's concentrate on the facts and make sure they stay in the forefront.

==> Were there break-ins involving the E911 system? If so, the entire story must be revealed. How did the hackers get in? What did they have access to? What could they have done? What did they actually do? Any security holes that were revealed should already have been closed. If there are more, why do they still exist? Could the original holes have been closed earlier and, if so, why weren't they? Any hacker who caused damage to the system should be held accountable. Period. Almost every hacker around seems to agree with this. So what is the problem? The glaring fact that there doesn't appear to have been any actual damage. Just the usual assortment of gaping security holes that never seem to get fixed. Shoddiness in design is something that shouldn't be overlooked in a system as important as E911. Yet that aspect of the case is being side-stepped. Putting the blame on the hackers for finding the flaws is another way of saying the flaws should remain undetected.

==> Under no circumstance should the Phrack newsletter or any of its editors be held as criminals for printing material leaked to them. Every publication of any value has had documents given to them that were not originally intended for public consumption. That's how news stories are made. Shutting down Phrack sends a very ominous message to publishers and editors across the nation.

==> Finally, the privacy of computer users must be respected by the government. It's ironic that hackers are portrayed as the ones who break into systems, read private mail, and screw up innocent people. Yet it's the federal authorities who seem to have carte blanche in that department. Just what did the Secret Service do on these computer systems? What did they gain access to? Whose mail did they read? And what allowed them to do this?

#### Take Exception

It's very easy to throw up your hands and say it's all too much. But the facts indicate to us that we've come face to face with a very critical moment in history. What comes out of this could be a trend-setting precedent, not only for computer users, but for the free press and every citizen of the United States. Complacency at this stage will be most detrimental.

We also realize that one of the quickest ways of losing credibility is to be

shrill and conspiracy-minded. We hope we're not coming across in this way because we truly believe there is a significant threat here. If Phrack is successfully shut down and its editors sent to prison for writing an article, 2600 could easily be next. And so could scores of other publications whose existence ruffles some feathers. We cannot allow this to happen.

In the past, we've called for people to spread the word on various issues. More times than not, the results have been felt. Never has it been more important than now. To be silent at this stage is to accept a very grim and dark future.

\*\*\*\*\*  
ARTICLE TWO: A REVIEW OF THE E911 DOCUMENT ITSELF  
\*\*\*\*\*

Documentation on the E911 System  
March 1988  
\$79,449, 6 pages  
Bell South Standard Practice  
660-225-1045V  
Review by Emmanuel Goldstein

It otherwise would have been a quickly forgotten text published in a hacker newsletter. But due to all of the commotion, the Bell South E911 document is now very much in the public eye. Copies are extremely easy to come by, despite Bell South's assertion that the whole thing is worth \$79,449.

While we can't publish the actual document, we can report on its contents since it's become a news story in itself. But don't get excited. There really isn't all that much here.

Certain acronyms are introduced, among them Public Safety Answering Point (PSAP), also known as Emergency Service Bureau (ESB). This is what you get (in telco lingo) when you dial 911. The importance of close coordination between these agencies is stressed. Selective routing allows the 911 call to be routed to the proper PSAP. The 1A ESS is used as the tandem office for this routing. Certain services made available with E911 include Forced Disconnect, Alternative Routing, Selective Routing, Selective Transfer, Default Routing, Night Service, Automatic Number Identification, and Automatic Location Identification.

We learn of the existence of the E911 Implementation Team, the brave men and women from Network Marketing who help with configuration in the difficult cutover period. This team is in charge of forming an ongoing maintenance subcommittee. We wouldn't want that juicy tidbit to get out, now would we?

We learn that the Switching Control Center (SCC) "is responsible for E911/1AESS translations in tandem central offices". We're not exactly shocked by this revelation.

We also find out what is considered a "priority one" trouble report. Any link down to the PSAP fits this definition. We also learn that when ANI fails, the screens will display all zeroes.

We could go on but we really don't want to bore you. None of this information would allow a hacker to gain access to such a system. All it affords is a chance to understand the administrative functions a little better. We'd like to assume that any outside interference to a 911 system is impossible. Does Bell South know otherwise? In light of their touchiness on the matter, we have to wonder.

We'd be most interested in hearing from people with more technical knowledge on the subject. What does this whole escapade tell us? Please write or call so the facts can be brought forward.

\*\*\*\*\*

2600 MAGAZINE WANTS TO HEAR YOUR THOUGHTS AS WELL AS ANY ADDITIONAL FACTS YOU MAY BE ABLE TO SHARE WITH US. POST PUBLIC COMMENTS HERE. YOU CAN SEND PRIVATE MAIL TO 2600@well.sf.ca.us OR 2600 EDITORIAL DEPARTMENT, P.O. BOX 99, MIDDLE ISLAND, NY 11953. IF YOU WANT TO CALL US, OUR PHONE NUMBERS ARE: (516) 751-2600 (VOICE/MACHINE) OR (516) 751-2608 (FAX).

\*\*\*\*\*

---

### **🚀 Crypto '90 conference, 11-15 August 1990, UC Santa Barbara**

*John Gilmore <gnu@toad.com>*

*Tue, 22 May 90 16:28:17 PDT*

Crypto '90 is the tenth in a series of workshops on cryptography, and is sponsored by the international Association for Cryptologic Research, in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy, and the Computer Science Department of the University of California, Santa Barbara. The program for the workshop will cover all aspects of cryptology. Extended abstracts of the papers presented at the conference will be distributed to all attendees at the conference, and formal proceedings will be published at a later date.

....more info from the brochure skipped...

Participation is invited by interested parties, but attendance at the workshop is limited, and pre-registration is required (\*there will be no registration at the door!\*). Campus accommodations will be available for participants who register by July 6, 1990. Cost for regular attendance is \$160, for Eurocrypt attendees \$120, for students \$100. Room and board runs \$260 for a single room or \$215/ea to split a double, or you can use a hotel and restaurants if you bring a car.

To get full info and registration form, talk to Sherry McMahan, Crypto '90, CYLINK, 130B Kifer Court, Sunnyvale, CA 94086 USA.

I went to this conference last year and had a very good time. I learned a lot, met a number of interesting people, and did some fun beachcombing. The story on no-at-the-door-registration last year was that they have to commit to exactly what facilities they'll use too early, since it's held in a campus rather than a hotel. Before I got there I figured it was so the spooks could check up on everybody :-).



Search RISKS using [swish-e](#)

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



Search RISKS using [swish-e](#)

# THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 9: Issue 96

Tuesday 29 May 1990

## Contents

- [Roller Coaster Accident Blamed on Computer](#)  
[Gary Wright](#)
- [ATMs robbed with no signs of tampering](#)  
[Stephen W Thompson](#)
- [Bank deposits huge amount in account and blames owner!](#)  
[Richard Muirden](#)
- [Risks in secure documents](#)  
[David Fuller](#)
- [You Think YOU Have Trouble with Your Telephone Company?](#)  
[Donald B. Wechsler](#)
- [Steve Jackson Games & A.B. 3280](#)  
[Brian Sherwood](#)
- [Re: Secure UNIX Infected?](#)  
[Steve Bellovin](#)  
[Henry Spencer](#)
- [Dereferencing Tim Kay's address](#)  
[David Kuder](#)
- [Info on RISKS \(comp.risks\)](#)

---

### ✂ Roller Coaster Accident Blamed on Computer

Gary Wright <[wright@hsi.com](mailto:wright@hsi.com)>

Tue, 29 May 1990 18:01:46 EDT

ACE News is the official newsletter of The American Coaster Enthusiasts. The following article appeared in ACE News, Volume XII, Issue 6, May 1990:

Worlds of Fun \_Timber\_Wolf\_ Incident Blamed on Computer

The 1990 season began inauspiciously for Worlds of Fun (Kansas City, MO) when two trains on the one-year-old \_Timber\_Wolf\_ (world class woodie) collided on opening day.

No one was seriously hurt in the March 31 crash, but nine of the 28 passengers

sent to the hospital were admitted, one with a broken leg. The ride was closed immediately after the incident.

The accident occurred when the computerized control system allowed one train to rear-end another on the first set of station brakes.

Beginning April 2, the \$3-million wooden coaster was subjected to an exhaustive investigation by Worlds of Fun, the Dinn Corporation (which built the coaster), the engineering firm Burns & McDonnell, and TechnoMation, an electronic systems integration design company.

Before Timber Wolf reopened to the public on April 27, the trains, structure, track and braking and computer systems were all thoroughly inspected. The ride also went through an extensive series of test runs with park executives aboard.

Timber Wolf is currently running with only one train. Two-train operation will begin as soon as a new, co-processing computerized control system is installed. With four times as many sensors as the original system (many of them redundant) and two computer controls instead of one, Worlds of Fun officials are confident that a similar accident will not occur.

[[RISKS-4.91](#) (28 May 1987) and ACM SIGSOFT Software Engineering Notes 12 3 (Jul 1987) relate a previous case of two roller coasters involved in a crash, in which electromagnetic radiation was suspected. PGN]

---

### **Automatic Teller Machines robbed with no signs of tampering**

"Stephen W Thompson" <[thompson@a1.quaker.upenn.edu](mailto:thompson@a1.quaker.upenn.edu)>  
Tue, 29 May 90 09:17:01 -0400

The Philadelphia Inquirer, in a story from Monday, 21 May 1990 by Maureen Graham and Mike Schurman headlined SHORE ATM TAPPED FOR \$100,000 reported that an automatic teller machine located in Trump Castle Casino Resort in Atlantic City, NJ (and owned by National Westminster Bank) was missing about \$100,000 which was apparently taken the previous week. The FBI was reportedly on the case, and was considering embezzlement, inaccurate or inadequate record keeping or theft by someone outside the bank.

There was no forced entry into the machine. The article indirectly quoted the bank's CEO L. Douglas O'Brien, reporting that "Bank officials said they believed that the thief had access to the bank's security system." The funds were discovered during a weekly audit of the machines. Two ATMs at other casino hotels had amounts of \$10,000 and \$20,000 stolen.

Some of the nitty gritty details:

"According to O'Brien, the money is delivered by bank employees, as needed, to the Trump Castle lobby MAC [Money Access Center] machine and placed in a vault inside the machine.

"The money from the vault is then transferred to canisters inside the machine by two employees -- from the bank or from a Philadelphia security

firm that services the bank on weekends and during non-banking hours.

"O'Brien said the \$100,000 was determined to be missing from the vault section of the MAC machine.

"To provide security, a dual-access system is used to service a MAC machine -- each employee has access to only half the security information required to enter the system.

"However, officials said they suspected one person bypassed the security system.

"It was a legal access. It was not forced open. The system was compromised," O'Brien said."

CoreState Financial Corp. operates the computer system for the machines.

\*\*\*\*\* End of article synopsis \*\*\*\*\*

In what may be a related development, I heard on the news this weekend of ATMs in New York city that had money stolen, again with no signs of tampering. There is no hard evidence that a computer RISK is involved in any of these thefts; other security breaches are as likely. The Inquirer article doesn't make clear what the "security system" consists of -- computer system or not? The tone of the article makes it sound as if the reporters suspected a computer RISK, but I can't always trust reporters' suspicions.

Steve Thompson, University of Pennsylvania, 215-898-4585 Standard Disclaimer

---

### **Bank deposits huge amount in account and blames owner!**

*Richard Muirden, A Star Trek Fan <s892024@minyos.xx.rmit.oz>  
Mon, 28 May 90 13:58:27+1100*

I thought this personal story might be of interest to RISKS readers:

In mid 1988 I had an interesting experience with my bank account - I had had \$87,889,984 (or some such random value in the \$87 million range!) added to my account!! On asking the bank concerned if they could fix the problem they blamed me for "Keying in the amount at an ATM!" Of course I protested my innocence - where would I get that sort of money from?! :-) Now I would have thought that surely:

- a) The ATM software would check for such obvious erroneous data if I had in fact entered such an amount as a deposit. (ever heard of range checking?!)
- b) With such large sums of money would the computer not alert an operator to check to see that it was valid (considering that I do not hold a corporate account).

The problem was fixed after several weeks (!) and although rather amusing {and

if only I got the interest on that money :-{ } to do an account balance and see a nice amount for a change :-) but it still leaves me wondering just what happened and why they should blame \*me\* for such an obvious computer error! Maybe it was because I am a student! I wonder if this kind of error has occurred to anyone else.

-Richard Muirden                      s892024@minyos.xx.rmit.OZ.AU

---

### **✦ Risks in secure documents**

*David Fuller <dafuller@sequent.UUCP>  
Sun, 27 May 90 20:49:59 -0700*

In response to your volume 9, Issue 94 observations regarding the security of "secure" documents, I offer some comments:

1) The best defense is naivety. Diamond brokers (at least used to) ship quantities of product via 1st class mail because it was reliable (in the States) and anonymous.

Perhaps our most secure documents should be published in the Consumer Information Catalog (available free from Pueblo, CO). Or perhaps they are; suitably encrypted to look like regular documents.

2) The congressional register, if it is difficult to analyse, possibly represents a chaotic system and models noise very well. Political statements excluded.

On other topics...

Another interesting thing. We had our building "fire alert" system go off the other day, fortunately a minor problem, and as we were watching the fire department do their thing (very well) a cohort asked about the policy regarding shutting down the machines in an emergency. I said that (in so many words) I thought the idea was to preserve human (not machine) lives. My workmate responded that his previous job was with a company whose policy was that machines must be safely shut down before humans could respond to such an emergency and insure personal safety.

Whether winding thread, sewing shirts or making steel, the organization has life greater than human's; still.

Dave

---

### **✦ You Think YOU Have Trouble with Your Telephone Company?**

*Wechsler, Donald B <m17434@mwvm.mitre.org>  
Tuesday, 29 May 1990 10:14:36 EST*

After entertaining many explanations for misrouted telephone calls, RISKS should consider another possibility. Last week, the Houston Post reported that Ginger was in the dog house with the Arlington, Texas, police department. The

Post continued:

That's because the Lhasa apso twice managed to place 911 emergency calls from an Arlington home. At least, police can think of no other explanation for the calls. Police said they found the dog beside a telephone when they entered the place after receiving the second call. No one else was home.

Ginger's owner, Jane Shumaker, said she hadn't programmed 911 into her telephone's automatic dialing system, and she finds it hard to believe her pet made the call. But she added, "I'm beginning to think she's smarter than I thought. Maybe she was lonesome."

Dare I mention it? It seems our phone system is going to the dogs.

[An Apso Facto case. Don't terrier hair out.  
The dog was doing a St. Gingervitus Dance. PGN]

---

### **Steve Jackson Games & A.B. 3280**

*Brian Sherwood <aha@m-net.ann-arbor.mi.us>  
27 May 90 03:50:07 EDT (Sun)*

> Computer Gaming World (Golden Empire Publications)  
> June, 1990, Number 72, Page 8  
> Editorial by Johnny L. Wilson

#### It CAN Happen Here

Although Nobel Prize-winning novelist Sinclair Lewis is probably best known for 'Main Street', 'Babbitt', 'Elmer Gantry', and 'Arrowsmith', my personal favorites are 'It Can't Happen Here' and 'Kingsblood Royal'. The latter is an ironic narrative in which who suffers from racial prejudice toward the black population discovers, through genealogical research, that he himself has black ancestors. The protagonist experienced a life-challenging discovery that enabled Lewis to preach a gospel of civil rights to his readership.

The former is, perhaps, Lewis' most lengthy novel and it tells how a radio evangelist was able to use the issues of morality and national security to form a national mandate and create a fascist dictatorship in the United States. As Lewis showed how patriotic symbolism could be distorted by power-hungry elite and religious fervor channeled into a political movement, I was personally shaken. As a highschool student, reading this novel, for the first time, I suddenly realized what Lewis intended for his readers to realize. "It" (a dictatorship) really CAN happen here, There is an infinitesimally fine line between protecting the interests of society and encumbering the freedoms of the self-same society in the name of protection.

Now it appears that the civil liberties of game designers and gamers themselves are to be assaulted in the name of protecting society. In recent

months two unrelated events have taken place which must make us pause: the raiding of Steve Jackson Games' offices by the United States Secret Service, and the introduction of A.B. 3280 into the California State Assembly by Assemblyperson Tanner.

On March 1, 1990, Steve Jackson Games (a small pen and paper game company) was raided by agents of the United States Secret Service. The raid was allegedly part of an investigation into data piracy and was, apparently, related to the latest supplement from SJG entitled, GURPS Cyberpunk (GURPS stands for Generic Universal Role-Playing System). GURPS Cyberpunk features rules for a game universe analogous to the dark futures of George Alec Effinger ('When Gravity Fails'), William Gibson ('Neuromancer'), Norman Spinrad ('Little Heroes'), Bruce Sterling ('Islands in the Net'), and Walter Jon Williams ('Hardwired').

GURPS Cyberpunk features character related to breaking into networks and phreaking (abusing the telephone system). Hence, certain federal agents are reported to have made several disparaging remarks about the game rules being a "handbook for computer crime". In the course of the raid (reported to have been conducted under the authority of an unsigned photocopy of a warrant; at least, such was the only warrant showed to the employees at SJG) significant destruction allegedly occurred. A footlocker, as well as exterior storage units and cartons, were deliberately forced open even though an employee with appropriate keys was present and available to lend assistance. In addition, the materials confiscated included: two computers, an HP Laserjet II printer, a variety of computer cards and parts, and an assortment of commercial software. In all, SJG estimates that approximately \$10,000 worth of computer hardware and software was confiscated.

The amorphous nature of the raid is what is most frightening to me. Does this raid indicate that those who operate bulletin board systems as individuals are at risk for similar raids if someone posts "hacking" information on their computer? Or does it indicate that games which involve "hacking" are subject to searches and seizures by the federal government? Does it indicate that writing about "hacking" exposes one to the risk of a raid? It seems that this raid goes over the line of protecting society and has, instead, violated the freedom of its citizenry. Further facts may indicate that this is not the case, but the first impression strongly indicates an abuse of freedom.

Then there is the case of California's A.B 3280 which would forbid the depiction of any alcohol or tobacco package or container in any video game intended primarily for use by minors. The bill makes no distinction between positive or negative depiction of alcohol or tobacco, does not specify what "primarily designed for" means, and defines 'video game' in such a way that coin-ops, dedicated game machines, and computer games can all fit within the category.

Now the law is, admittedly, intended to help curb the use and abuse of alcohol and tobacco among minors. Yet the broad stroke of the brush with which it is written limits the dramatic license which can be used to make even desirable points in computer games. For example, Chris Crawford's 'Balance of the Planet' depicts a liquor bottle on a trash heap as part of a screen talking about the garbage problem. Does this encourage alcohol abuse? In 'Wasteland', one of the encounters involves two winos in an alley. Does their use of

homemade white lightning commend it to any minors that might be playing the game?

One of the problems with legislating art is that art is designed to both reflect and cast new light and new perspectives on life. As such, depiction of any aspect of life may be appropriate, in context. Unfortunately for those who want to use the law as a means of enforcing morality, laws cannot be written to cover every context.

We urge our California readers to oppose A.B. 3280 and help defend our basic freedoms. We urge all of our readers to be on the alert for any governmental intervention that threatens our freedom of expression. "It" not only CAN happen here, but "it" is very likely to if we are not careful.

---

### **✉ Re: Secure UNIX Infected?**

<*smb@ulysses.att.com*>

*Sat, 26 May 90 16:41:55 EDT*

If you read between the lines you will note that a development version of AT&T UNIX was infected. The message is that the "NCSC" is more concerned about "confidentiality" than, say, integrity. The sooner we get a counter balance to the NCSC critical mass within POSIX P1003.6 (security) the better our future.

[description of Duff's virus deleted]

he loosed the thing inside AT&T as an experiment to see how well such a weak virus would spread, and how it could be started. (he started the infection by adding an infected copy of "echo" to some public directories he had write access too).

[more deletions]

it caused some particular problems on a "secure" unix that was being developed, since the kernel detected the attempts of the virus to propagate, and killed the virus.

I think there's a serious misconception here about Duff's virus, where it spread, and "AT&T UNIX". There are no lines to read between; what was said is literally and completely true, with no hidden messages. Tom's virus was developed on 9th Edition UNIX systems, a research version that bears little relation to System V or anything else in the product line. No "development version" of the UNIX system was affected. This is doubly true of AT&T's secure UNIX system product (System V/MLS), which has been certified at the B1 level. The "secure unix" affected was an experimental implementation of mandatory access controls, using a modified 9th Edition kernel. And, as noted, even the affected system was still under development at the time -- hardly a fair criticism of any finished system.

All that aside, I wouldn't be so quick to dismiss the NCSC's efforts as focused on confidentiality rather than integrity. While there certainly is that bias, there's a lot to be said for maintaining confidentiality even in the commercial world (as numerous stories in RISKS attest, of course). And, at least for some programs, the mandatory access controls can be used to maintain integrity: mark any critical program as being in the lowest-possible security level, lower than any user process. That way, any attempt to modify the program appears to be an access-control violation.

And there's one more point that shouldn't be ignored. The Orange Book does not simply list a set of features. It describes a development process, an attitude towards software management, and (to some extent) an enforced modularity. All of these contribute to reliable -- and hence secure -- software. Furthermore, the certification process itself is quite stringent. There's a world of difference between, say, ``B1- certifiable" -- which generally means a feature list -- and ``B1 certified."

If there are specific features you'd like to see added to POSIX for better integrity maintenance, by all means propose them. But as far as I can tell, the NCSC -- and its sponsor, DoD -- are among the few groups that not only take security seriously, but are prepared to put their money where their mouth is.

--Steve Bellovin

---

### **✂ Re: Secure UNIX Infected?**

*<henry@zoo.toronto.edu>*

*Mon, 28 May 90 12:11:35 EDT*

>If you read between the lines you will note that a development version of AT&T  
>UNIX was infected. The message is that the "NCSC" is more concerned about  
>"confidentiality" then, say, integrity. The sooner we get a counter balance to  
>the NCSC critical mass within POSIX P1003.6 (security) the better our future.

If you read the Usenix paper referred to, you will find out that (a) the secure Unix in question is a research system, not a product or potential product, and (b) as mentioned in the Risks posting, the virus infected it at a time when much of the security had not yet been turned on. I would urge people to read the paper before jumping to unwarranted conclusions.

Henry Spencer at U of Toronto Zoology

uunet!attcan!ut zoo!henry

---

### **✂ Dereferencing Tim Kay's address**

*David Kuder <david@indetech.com>*

*Sun, 27 May 90 20:39 PDT*

When Tim first wrote about his problems I thought that they were related to the fact that zipcodes don't provide a functional dependency for city and state. That is, more than one city (well wide spot in the road) can be in one zip code. This problem has bitten my father who

now has subscriptions with a 4 line address of the form:

Doc Kuder  
3 Elm St.  
Brownsville  
Emmittsburg, PA 18888

Because there is an Elm Street in both Brownsville and Emmittsburg and they've got nothing to do with each other, but the Post Office insists that 18888 is Emmittsburg.

I also thought that Tim's problem might be that the zip code he's using is only for the dorms at Caltech. The rest of campus has its own zip code, and the box number Tim uses doesn't match dorm practice. It shouldn't matter since both zip codes go to the same campus Post Office. When I first moved off campus, I used the campus zip code and had my delivered even slower than normal since it was sent to campus first then bounced. That house has since become part of campus -- I wonder what it's zip code is now?

Tim's problem is actually "Box". A quick scan of the zip code directory shows that only post office boxes in Pasadena can be found in zip code 91102. I suggest that Tim use something like "Building" or "Mailstop". The campus Post Office may be able to give him the definitive answer.

David A. Kuder

david@indetech.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 9: Issue 97**

**Wednesday 30 May 1990**

## Contents

- [The C3 Legacy, Part 6: Feedback](#)  
[Les Earnest](#)
- [Re: You Think YOU Have Trouble with Your Telephone Company?](#)  
[Rodney Hoffman](#)
- [Right to Privacy, Public Funds, and the 2600](#)  
[Bob Estell](#)
- [Re: Steve Jackson Games & A.B. 3280](#)  
[Chuq Von Rosbach](#)
- [Re: ATMs robbed with no signs of tampering](#)  
[Bob Campbell](#)
- [Re: ATMs robbed in Trump Castle](#)  
[Avi Belinsky](#)
- [Re: Secure UNIX Infected?](#)  
[Mark Gabriele](#)
- [Info on RISKS \(comp.risks\)](#)

---

### **✉ The C3 Legacy, Part 6: Feedback**

*Les Earnest* <LES@SAIL.Stanford.EDU>  
30 May 90 1036 PDT

[My apologies for the gap in this series -- I'm running for City Council currently and don't seem to have enough spare cycles. -Les]

Was there ever a command and control system that worked?

My opening remark in [RISKS 9.80](#) was: "Of the dozens of command and control system development projects that were initiated by the U.S. Air Force in the early 1960s, none appeared to perform its functions as well as the manual system that preceded it." Gene Fucci, who worked on the Air Force satellite surveillance programs as a project engineer on SAMOS and later as Field Force Test Director of MIDAS, found my remarks "somewhat distorted" in that he believes the satellite command and control systems worked well.

I will plead relative ignorance of those systems, but note that they were called just "control systems" until "command and control" became a buzzword in the early 1960s. I do not wish to take the position that all systems to which the term "command and control" or "command-control-communications" was eventually applied were failures -- just that all of the dozens that I knew of were failures.

#### SAGE revisited

Some of the earlier C3 Legacy postings on SAGE have found their way via a circuitous route to an old friend of mine, Phil Bagley, who also helped design that system. Phil has now sent me snail-mail that takes a different view of that program, as follows.

"I think that you have discovered what is behind the curtain. In case you haven't, let me tell you my view. The motivation behind a big military electronic system such as SAGE or BMEWS is not to have it work. It is just to create the illusion that the sponsor is doing his job, and perhaps peripherally to provide an opportunity to exercise influence. Lincoln Lab and MITRE had no motivation to point out the obvious -- that the emperor had no clothes. If you had asked a responsible think tank who had no stake in the outcome how to deal most effectively with the issues, you would have recommendations very different from those that guided the electronic systems developments.

"Now it wasn't all for naught. Out of SAGE, computer technology got a big boost. IBM learned how to build core memories and made a lot of money building machines with core memories. Lots of people like you and me got good systems and programming training (I still write programs). Ken Olson learned how to design digital equipment and ultimately gave the world a few billion dollars worth of Vaxes.

"The moral of all this is: When things appear not to make sense you very probably are looking at it from the 'wrong' point of view. Another way to say it: It's pretty hard to fool Mother Nature, so if it appears that she is being fooled, try to find a point of view which doesn't imply that she's being fooled."

While Phil and others may be comforted by this view, I will argue that it amounts to nothing more than "Whatever is, is right," which grates on my rationalist soul. I believe that if a comparable amount of government money had been invested in research, or on a more tractable application, that computer technology would have advanced much more quickly than actually happened.

I believe that as soon as MIT and MITRE engineers figured out that they had designed an unworkable system, they had an ethical obligation to point that out to their sponsors. Instead they (we) helped perpetuate the myth that it worked so that we could continue in our beloved technological lifestyle.

Phil's mention of Ken Olson reminds me that we gave a going-away party for him and Harlan Anderson at the MIT Faculty Club when they left to form

their company to make transistorized digital modules based on experience in building the TX-0 and TX-2 computers at Lincoln Lab. We told them that they could have their old jobs back after their start-up went belly-up, as we all expected. In fact, that reportedly came rather close to happening more than once in the first couple of years, but somehow DEC squeaked through and grew a bit.

Requiem: the SAIL computer, which would have reached the grand old age of 25 next week, is slated to retire tonight and die in the near future. It has provided an intellectual home for a very productive generation of researchers and will be remembered fondly.

(Next part: the Foggy Bottom pickle factory)

-Les Earnest (Les@Go4.Stanford.edu)

---

### ✂ You Think YOU Have Trouble with Your Telephone Company?

Rodney Hoffman <Hoffman.ElSegundo@Xerox.com>  
30 May 90 12:58:31 PDT (Wednesday)

[Admittedly tangential, but fun....]

[Oh, yes, this is a VERY OLD shaggy dog story, but worth retelling. It might even have appeared in RISKS before, but I don't recall it. On the other hand, this time I do not feel like grepping my way through the archives. Apologies to those of you to whom it rings true. PGN]

Donald Wechsler's story in [RISKS 9.96](#) (about the Lhasa apso which may have learned to dial 911) reminded me of one of my favorite stories. I found it in "Computers and Society Digest", Number 39, Tuesday, September 9th 1986. As you can see below, it is said to have originated in 1977.

. . . . .

Date: Mon, 8 Sep 86 16:03:35 PDT  
From: Dave Taylor  
Subject: Interesting Phone Calls

#### AN UNUSUAL TELEPHONE SERVICE CALL

This story was related by Pat Routledge of Winnepeg, ONT about an unusual telephone service call he handled while living in England.

It is common practice in England to signal a telephone subscriber by signaling with 90 volts across one side of the two wire circuit and ground (earth in England). When the subscriber answers the phone, it switches to the two wire circuit for the conversation. This method allows two parties on the same line to be signalled without disturbing each other.

This particular subscriber, an elderly lady with several pets called to say

that her telephone failed to ring when her friends called and that on the few occasions when it did manage to ring her dog always barked first. Torn between curiosity to see this psychic dog and a realization that standard service techniques might not suffice in this case, Pat proceeded to the scene. Climbing a nearby telephone pole and hooking in his test set, he dialed the subscriber's house. The phone didn't ring. He tried again. The dog barked loudly, followed by a ringing telephone. Climbing down from the pole, Pat found:

- a. Dog was tied to the telephone system's ground post via an iron chain and collar
- b. Dog was receiving 90 volts of signalling current
- c. After several jolts, the dog was urinating on ground and barking
- d. Wet ground now conducted and phone rang.

Which goes to prove that some grounding problems can be passed on.

This anecdote excerpted from Syn-Aud-Con Newsletter, Vol 4, No 3, April 1977.

---

### ✂ Right to Privacy, Public Funds, and the 2600 [[RISKS-9.95](#)]

"FIDLER::ESTELL" <estell%fidler.decnnet@scfd.nwc.navy.mil>  
30 May 90 08:41:00 PDT

There is a dual standard of conduct, of ethics, for managing money: One for private funds, and another, higher standard for "public money." All of us who spend public money, collect it, live on it, are called to an ethic described, by Shakespeare I believe, for Caesar's wife, to be "above suspicion."

The rule is simple: If you choose to live by your wits, and to be "sharp" in your professional practices [i.e., bend rules that are flexible, cut corners that "don't seem to matter"], then do it with private funds.

The backbone of the InterNet is publicly funded. Period. Many of the host computers on the InterNet are publicly funded. Thus, I have always assumed that the traffic was monitored from time to time. Some of us have taken advantage of that to bring issues to the attention of the monitors, without having to find explicit US Mail addresses for them.

All who benefit from the privilege - "PRIVILEGE," NOT "RIGHT" - of spending public money must be even more prudent with that public money than with our private funds. So many have gotten "the top of the line model" because it was available; in private life - REAL life - we often choose some lesser model, because it is prudent to compromise. [Else we would all be driving Cadillac, BMW, Mercedes, Mazda, or some other very fine automobiles, instead of the Fords and Chevrolets and other good, but not excellent, cars we do.]

I recently wrote a US Senator with an idea for capital gains tax breaks. In part, I suggested that the US make intelligent decisions about which industries to encourage, rather than offering tax benefits for any investment held over some period of time. An approximate quotation of my rational summarizes my belief: " We should probably not give capital gains tax breaks for investments in Jack Daniels, and Playboy. I may choose to spend my private dollars that

way, but I don't want my tax dollars spent that way."

The US Mail (postal service), once part of government, is now said to be a "private corporation" with some special management by the executive branch, with Congressional oversight - but different in kind and degree from either the old or new "AT&T." In any case, users are said to pay, at the time, for services rendered, one letter or parcel at a time. Even so, there are regulated - forbidden - uses of the mails, aside from and in addition to the privacy aspects.

We must appreciate the old maxim that "Your right to swing your fist ends at the tip of my nose." The 2600 gang needs to understand the computer corollary of that; and, as they say, we all need to understand the risk that nontechnical zealots will over legislate to protect their noses.

Bob

---

**✉ Re: Steve Jackson Games & A.B. 3280 (Sherwood, [RISKS-9.96](#))**

<chuq@Apple.COM>

30 May 90 05:15:22 GMT

A couple of points that aren't in this report. According to reports I've seen elsewhere, the person working on for Jackson Games was a former Legion of Doom member, who was also working on a book of interviews of Doom members. If what I just said actually is true, having a known hacker writing a 'manual' on hacking, even a fictional one, is something the Secret Service would want to keep an eye on -- imagine, for instance, that the fictional game instructions are actually true and the supplement was published as a way of passing them around in a covert way.

Now, everything I've heard indicates this isn't what happened: it really is fictional material. But it's an interesting concept in theory.

> The amorphous nature of the raid is what is most frightening to me. Does  
>this raid indicate that those who operate bulletin board systems as individuals  
>are at risk for similar raids if someone posts "hacking" information on their  
>computer?

If you're running a BBS that's supporting a group of system crackers, you are, at least, contributory to felony crimes. Sure you should worry about someone knocking on your door. A BBS that's on the up-and-up should have no worries, though.

>Or does it indicate that games which involve "hacking" are subject  
>to searches and seizures by the federal government? Does it indicate that  
>writing about "hacking" exposes one to the risk of a raid? It seems that this  
>raid goes over the line of protecting society and has, instead, violated the  
>freedom of its citizenry.

Not if the Legion of Doom angle is true. This is not to imply that Steve Jackson or Jackson games was at all involved with any Doomers, but moire likely stuck in the middle.

Chuq Von Rospach <+> chuq@apple.com <+> [This is myself speaking]

---

**⚡ Re: ATMs robbed with no signs of tampering**

*Bob Campbell <campbelr@hpclad0.cup.hp.com>*

*Wed, 30 May 90 17:04:59 pdt*

I recently had a chance to inspect the back of an automated teller while conducting some business with the human teller that works part-time on site.

It was divided into three sections, the computer, the records and the money. I noticed that one section had both combination and key locks and was informed that it contained the money. The section housing the computer was defended by a simple key lock.

I pointed out that Hewlett Packard was filled with people who design and build computers as well as equipment to monitor and test computers she noted that her teenage son thought it was a risk, but the bank considered the money quite safe.

Now if the lock manufacturer can make a key from lock number and type . . .

Bob Campbell, Hewlett Packard

---

**⚡ ATMs robbed in Trump Castle (Re: [RISKS-9.96](#))**

*Avi Belinsky <abelinsk@sunee.waterloo.edu>*

*Wed, 30 May 90 10:44:02 EDT*

>"It was a legal access. It was not forced open. The system was

^ ^ ^ ^ ^

>compromised,' O'Brien said."

Legal in the syntactic sense perhaps, but surely not in the legal sense. Yet another example of when computer jargon crosses the boundary into everyday speech.

Avi

---

**⚡ Re: Secure UNIX Infected? (Bellovin, [RISKS-9.96](#))**

*Mark Gabriele <gabriele@riverdale.toronto.edu>*

*Wed, 30 May 90 15:20:14 EDT*

smb@ulysses.att.com writes:

> There's a world of difference between, say, ``B1- certifiable" -- which  
> generally means a feature list -- and ``B1 certified."

I'd like to state for the record that what the NCSC does is NOT product "certification", but product "evaluation". Certification refers to a specific site being approved (usually by an authority referred to as a DAA, or Designated Accrediting Authority) as "B1 (or whatever digraph) secure". This certification may be contingent upon posting armed guards at every door to identify users instead of including a user authentication mechanism in the system, or any other restrictions the DAA feels are appropriate. An NCSC evaluation, on the other hand, is based upon the TCSEC requirements exclusively. A product must meet all of the requirements for a candidate class in order to receive that rating; there is no bargaining with the requirements based upon the judgement of a DAA. Thus, an \*evaluation\* of a system is generally more stringent than a certification, because the evaluation process tends not to allow a procedural correction for a deficiency in the hardware and software elements of the system.

Mark Gabriele (gabriele@hub.toronto.edu)



Search RISKS using [swish-e](#)

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