

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 8**

# Friday 30 June 1989

# Issue 1 (4 Jan 89)

- A Danish Home Companion (Hugh Miller)
- Tales from the Vincennes tape (Rodney Hoffman)
- Suit filed to force FBI to enforce privacy provisions of ECPA (John Gilmore)
- moRe: Armed with a keyboard ... -- Kevin Mitnick (Rodney Hoffman)
- Computer Chaos Congress 88 report (Klaus Brunnstein)
- Two steps forward, one step back (Jerry Leichter)
- Clapham Junction train crash (Clive Feather via Mark Brader)

# Issue 2 (4 Jan 89)

- Christmas 1988 Decnet Worm -- Counteracted (Cliff Stoll)
- Vincennes and the computer (Steve Philipson, Clifford Johnson)
- <u>Viruses and System Security (a story) (by Dave Platt, submitted to RISKS from rec.humor.funny by Jim Horning and Mark Brader)</u>
- Stallman, Minsky and Drescher on the Internet Worm (via Martin Minow)
- FAA Orders Computer Card Security Systems at 270 Airports (Henry Mensch)

#### Issue 3 (8 Jan 89)

- Computer-related accidental death (Gegg)
- Re: Danish Home Companion, Kierkegaard, and Feynman (David E. Leasure)
- "NO CARRIER" (Jef Poskanzer via David Sherman)
- Re: Tales from the Vincennes tape (Maj. Doug Hardie)
- "Hand-written" letters (Gary Chapman)
- Dark Side Hacker, an Electronic Terrorist (Rodney Hoffman)
- The risks of trusting CBS (Phil Goetz)
- Hackers pure and simple (Travis Marlatte)
- Viruses of all kinds (Travis Marlatte)
- Henry Cox's "Supercomputer used to `solve' math problem" (John C. Bazigos)

# Issue 4 (11 Jan 89)

- M1 Plane crash (Nigel Roberts)
- \$4.5 M Child Support Computer to be Scrapped in VA (Dave Davis)
- Eelskin wallets erase mag strips? (Jane D. Smith)
- Firearms Arrive in the Electronics Age (Allen)

- Unused city computer system set aside after 4 years, \$4M (Stephen W. Thompson)
- Re: Hackers' Conference versus CBS (John Gilmore)
- Issue 5 (11 Jan 89)
  - Digital Photos and the Authenticity of Information (Dave Robbins)
  - Medical software (Ivars Peterson via Robert Morris)
- Issue 6 (12 Jan 89)
  - Computers and Civil Liberties, article by Gary Marx (Ronni Rosenberg)
  - Losing systems (Vince Manis)
  - Our blinders [with respect to RISKS] (Don Alvarez)
  - Totally secure MAIL & infallible aeroplane warning systems (Nigel Roberts)
  - "Disaster Becomes a Matter of Routine" (Steve Philipson)
  - Re: Biased coverage of hacker's convention by CBS (Richard Thomsen)
  - SAFECOMP89 (Udo Voges)
  - Name this book -- for a box of cookies! (Cliff Stoll)
- Issue 7 (15 Jan 89)
  - Re: Medical Software (Are computer risks different?) (Jon Jacky)
  - Ground proximity warning (Bill Standerfer via Mark Brader)
  - Aircraft (Dale Worley)
  - You don't know what you've got till it's gone. (Phil Agre)
  - Data integrity (Brent Laminack)
  - Quality of Evidence (Bill Murray)
  - D.Robbins' conclusions (Authenticity of Information) (Allan Pratt)
  - · Risks of trusting the press (Brad Templeton)
  - Risks of Remote Student Registration: Another Interaction Story (Gary McClelland)
  - Medical information systems (Jerry Harper)
- Issue 8 (15 Jan 89)
  - Re: Losing systems -- and Structured Programming (Bruce Karsh)
  - Ethics of the Internet Request for Comments (Cliff Stoll)
  - Chaos Computer Congress 1988 -- Documentation (Klaus Brunnstein)
- Issue 9 (17 Jan 89)
  - Re: Structured Programming (Jim Horning, Steve Bellovin, Brian M. Clapper)
  - Re: Losing Systems (David Marks)
  - A risk averted (Gideon Yuval)
  - Re: M1 Crash -- Risks of misunderstood statistics (Jordan Brown)
  - Hacker wants to marry his computer (Cliff Stoll)
  - Hackers break open US bank networks (Dave Horsfall)
  - National Research Network (Brad Blumenthal)
  - Once-writable storage (Steve Philipson)
- Issue 10 (18 Jan 89)
  - Speak nicely to your air hostess or be blacklisted... (HCART)
  - (Too) Intelligent Network News mailing (Ralph A. Shaw)
  - Information protection in Europe (Steve Bellovin)
  - Re: Losing systems -- and Structured Programming (Henry Spencer, Lynn R Grant, Steven C. Den Beste)
  - Re: Ground proximity warning (Henry Spencer)
  - WORM storage and archival records (RAMontante)

- Re: 3 vs. 2 engined airplanes (Steve Jay)
- Re: Hackers break open US bank networks (Jan Wolitzky)
- Evidence (Bill Murray)

#### Issue 11 (19 Jan 89)

- Risks of no backup systems for critical applications (Yoram Eisenstadter)
- Computer malfunction downs traffic lights, one killed, one injured (Scott Campbell)
- Chaos Theory Predicts Unpredictability (PGN)
- China accused of software piracy (PGN)
- Friday the 13th Again (PGN)
- Computer error locks out politicians (D. Steele)
- Re: Losing Systems (Jerome H. Saltzer)
- Technical brilliance v. commercial acumen (Jerry Harper)
- National Credit Information Network (Sidney Marshall)
- Re: Ethics of the Internet (John Gilmore)
- RISKs of reading newspapers: Credit card fraud is not hacking. (Mike Van Pelt)
- Counting engines (Don Alvarez)

#### Issue 12 (20 Jan 89)

- Risk of using your own name (Gary T)
- Risks in NBS time by radio (computer malfunction downs lights) (Clements)
- Computer-related accidents in British chemical industry (Jon Jacky)
- Re: Losing Systems (Henry Spencer, Donald Lindsay, Keane Arase)
- · Failure of Software Projects (WHMurray)
- Re: Structured Programming (David Collier-Brown, Jerry Schwarz)
- Discrete probability and airplanes (Mike Olson)
- Re: Chaos theory (Phil Goetz)

#### Issue 13 (22 Jan 89)

- Gigabit superhighway/worms (Vint Cerf)
- IAB Ethics DRAFT (Vint Cerf)
- Space shuttle computer problems, 1981--1985 (Jon Jacky)
- F-16 that can't stall falls from sky (Scot E Wilcoxon)
- Re: China accused of software piracy (Jim Olsen)
- Losing systems (Dale Worley, Chris Lewis)
- Re: Structured Programming (John Mainwaring, Mark Rosenstein, Steve Pozgaj)

#### Issue 14 (24 Jan 89)

- Re: Medical Software -- testing and verification (Dave Parnas)
- NSA and the Internet (Vint Cerf)
- Re: Losing systems (Geoff Lane)
- Computer Emergency Response Team (CERT) (Brian M. Clapper)
- Probability and Product Failure (Geoff Lane) [lack of independence]
- Probabilities and airplanes (Robert Colwell, Mike Olson, Dale Worley)

## Issue 15 (25 Jan 89)

- More video piracy (Dave Curry)
- Computerized records of employee informers (Mike Trout)
- Censorship and computers (Anthony Finkelstein)
- Re: Object Oriented Programming (Benjamin Ellsworth)
- Structuring large systems (John Spragge)

About non-redundant redudant systems (Elizabeth D. Zwicky)

- Engine-count and the Spirit of St. Louis (Michael McClary)
- Counting engines (Jordan Brown)
- Re: Space shuttle computer problems, 1981--1985 (Henry Spencer)
- Revised Computer Ethics Course Proposal (Bob Barger)

#### Issue 16 (26 Jan 89)

- Cable video piracy (anonymous)
- F-111 downed by EMI? (Gordon Davisson)
- F-16 that can't stall falls from sky (Mike Tanner)
- Re: Probability and Product Failure [common mode failures] (Bruce Hamilton)
- Discrete probability and airplanes (Dave Settle)
- Micro-cellular phones (Steven C. Den Beste)
- Looking for Computer Folklore (Karla Jennings via Vernard C. Martin)

#### Issue 17 (27 Jan 89)

- ELIZA and Joe Weizenbaum (Bard Bloom)
- Savings, Loans, and Easy Money (PGN)
- Risks of inept management ["Losing Systems"] (John R. Levine)
- MIT Athena Kerberos Authentication System available for FTP (John Kohl via Jon Rochlis)
- Single-engine planes (Phil Karn)
- Multi-engine airplanes (Craig Smilovitz)

## Issue 18 (30 Jan 89)

- Hong Kong computer horse betting (George Moore)
- Keycard badges vs. anti-shoplift systems (Bruce Hamilton)
- Bank Fraud (Peter Golde)
- Crashing a PDP-11/40 (Computer Folklore) (Jeff Makey)
- Sprint to the Finish? (Steve Philipson)
- Information Security/Computer Crime Statistics (Stan Stahl)
- Re: ELIZA and Joe Weizenbaum (Bernie Cosell, Bob Krovetz)
- Virus conference hosts software swap meet (Robert Lee Wilson Jr)
- Structured Programs, Project Failures (Charles J. Wertz)
- Losing Systems (Mike Albaugh)

## Issue 19 (1 Feb 89)

- Massachusetts limits disclosure of driver's license database. (Jon Jacky)
- Dead Code Maintenance (Douglas Jones)
- Re: Structured Programming (Eric Roskos)
- Random Thoughts on Redundancy (Earl Boebert)
- One last word about probabilities (Dr Robert Frederking)
- Independence and probabilities (PGN)
- Counting Engines (Mike Bell)
- Talk by Roy Saltman on computerized vote tallying (Charles Youman)

## Issue 20 (5 Feb 89)

- FAA and flying under pressure in Alaska (PGN)
- New use for Credit Cards (?) (Leslie Chalmers)
- Computer Chaos in Burnaby (Stuart Lynne)
- Swedish fighter plane crash (Otto J. Makela)
- Re: Massachusetts limits disclosure of driver's license database. (Jerome H Saltzer)

"Computer Literacy Education" Report Available (Ronni Rosenberg)

- Engineering vs. Programming (Lynn R Grant)
- Re: Structured Programming (Al Arsenault, Allen Gordon, Dan Franklin)

#### Issue 21 (5 Feb 89)

- 'User friendliness' tradeoffs can lead to total nonsecurity (Eric S. Raymond)
- Capturing a password (Phil Karn)
- Collisions in DES (Jean-Jac. Quisquater)
- Re: Crashing a PDP-11/40 [static electricity] (Jeffrey Mogul)
- ATM error (Douglas Jones)
- Anecdotes: ping-pong robot; CCC breaks net (Konrad Neuwirth)
- Reguest for information: Health Hazards of Office Laser Printers (Keith Dancey)
- Re: Structured Programming (Michael J. Chinni)

# Issue 22 (8 Feb 89)

- B-1B bomber avionics problems (Jon Jacky)
- Risks of public terminal rooms (Roy Smith)
- Using barcodes for road toll payments (Phillip Herring)
- ATM error in Europe (John O'Connor)
- Computing as a Discipline (Peter J. Denning)
- Cryptic status displays, and GIGO (Mark Brader)
- Re: 'User friendliness' and forgotten root passwords (Shannon Nelson, Ge' Weijers, smv)
- Health Hazards of Office Laser Printers (Hal Murray, Jeffrey Mogul)
- Re: Keycard badges vs. anti-shoplift systems (Craig Leres)

## Issue 23 (9 Feb 89)

- Self-Taught Space Craft (Brian Randell)
- Still a few bugs in the system, as they say (Mark Brader)
- Multi-gigabuck information "theft" (Mark Brader)
- Risks of letting key people leave employment? (David A. Curry)
- Phone Risks (Greeny)
- Virus Technical Review (David J. Ferbrache)
- Re: WORM storage and archival records (Curtis Abbott)

# Issue 24 (13 Feb 89)

- Massive counterfeit ATM card scheme foiled (Rodney Hoffman, PGN)
- Computer blamed for 911 system crash (Rodney Hoffman)
- Risks of Selective Service (Rob Elkins)
- Re: Engines and probabilities (Barry Redmond, Robert Frederking)
- Re: Structured programming (Jim Frost)
- Re: Engineering vs. Programming (John Dykstra, Henry Spencer, Robert English, Shawn Stanley)

#### Issue 25 (14 Feb 89)

- Authenticity in digital media -- electronic time travel (Steve Philipson)
- Bogus Frequent Flyer Scheme (Kenneth R. Jongsma [and Dave Curry])
- · Automatic targeting for Maverick missile (Jon Jacky)
- Economics, Engineering and Programming (Jerry Leichter)
- RE: ATM Error in Europe (Udo Voges)
- Another bank error (Hsiu-Teh Hsieh)
- Static Electricity crash (Seth K)
- Legal clamp-down on Australian "hackers" (Neil Crellin)

MIT virus paper available for anonymous ftp (Jon Rochlis)

• Prospectus for "Computer Viruses" (J Cordani)

## Issue 26 (15 Feb 89)

- "\$15 Million Computer Dud Baffles Udall" (Joseph M. Beckman)
- Re: Computer blamed for 911 system crash (Rodney Hoffman, Paul Blumstein)
- Selling who-called-the-800-number data (Bob Ayers)
- PIN? Who needs a PIN? (Alan Wexelblat)
- Door Sensors and Kids (Eddie Caplan)
- Risks of misunderstanding probability and statistics (Tom Blinn)
- Why you can't "flip" bits on a WORM disc (Daniel Ford)
- Credit Checker & Nationwide SS# Locate (David Andrew Segal)
- Re: Authenticity in digital media (Pete Schilling)
- Re: multi-gigabuck information "theft" (Jeff Makey)

#### Issue 27 (16 Feb 89)

- FBI NCIC Data Bank (Bob Morris)
- Internet mail forgery (Walter Roberson)
- Re: Dead code maintenance (Clifford Johnson)
- Probabilities and Engines (Steve Philipson, Robert Dorsett, Daniel A. Graifer)

# Issue 28 (19 Feb 89)

- Continuing problems with WWMCCS command-and-control network (Jon Jacky)
- US missile-warning radar endangers friendly aircraft (Jon Jacky)
- Power failure problems (John Sinteur)
- The Risks of Going on Vacation (Jim Carson)
- Re: Faking Internet mail (Peter Scott)
- Multi-gigabuck value of information theft denied (Mark Brader)
- Re: multi-gigabuck information "theft" (David Chase)
- Re: Authenticity in digital media (Doug Krause)
- Digital doctoring of images (Richard Wiggins)
- PIN? Who needs a PIN? (Bill Mahoney)

# Issue 29 (22 Feb 89)

- Overloaded computer delays (overworked) commuters (Steve Graham)
- Chicago Phone Freak Gets Prison Term (Patrick Townson via Cliff Stoll)
- Computer Confinement (Joseph M. Beckman)
- Police officers sentenced for misuse of PNC (Nigel Roberts)
- The word "virus" causes panic (Nigel Roberts)
- Re: Faking Internet mail (Steve Bellovin, Kevin S. McCurley)

## Issue 30 (24 Feb 89)

- "Do you know who's reading your medical records?" (PGN)
- Wells Fargo ATM outage (PGN)
- New York 540 Phone Number Scam (John Murray)
- 900 "confession" number (Randal L. Schwartz)
- Re: Chicago Phone Freak Gets Prison Term (Rich Salz)
- Reach Out and Spy on Someone (Peter Scott)
- Power failure problems (Jonathan I. Kamens)
- Photographs as evidence (re: digital editing, etc.) (Ernest H. Robl)
- Stanford and rec.humor.funny (Martin Minow)

# Issue 31 (27 Feb 89)

- Bank fraud was "easy" (Stephen Page)
- Men accused of 'hacker' crime (Michael C Polinske)
- Stanford bboard censorship (Les Earnest, John McCarthy, Jerry Hollombe)
- Computer writing coach / friend (Rodney Hoffman)
- British Computer Society policy on safety-critical systems (Martyn Thomas)
- Reach out and spy (gls)
- Risks of Running a Hotel (Chuck Weinstock)
- Singing in the Rain (Kent Borg)
- [RISKS BARFMAIL] (PGN)

# Issue 32 (1 Mar 89)

- RISKS-LIST: On Risks of Running RISKS (PGN)
- Gripen prototype crash (Dave Newkirk, Kenneth R. Jongsma, Karl Lehenbauer)
- A pilot's account of a multi-engine failure (Karl Lehenbauer)
- Knowing probability just doesn't make a difference (Sumit Dongre)
- A new ATM risk: bureaucracy (Laura Halliday)
- IBM's claims for error-free code (Robert Lee Wilson Jr)
- Re: discussion of computer viruses (Brent Laminack)
- Re: [RISKS BARFMAIL] (Robert J. Reschly Jr.)

### Issue 33 (2 Mar 89)

- Viruses and the comics (Jack Holleran, Hope Munro)
- Hacking in the movies -- Working Girl (Martin Minow)
- Re: British Computer Society policy statement (Clifford Johnson)
- Hacking and Computer Fraud in the U.K. (Brian Foster)
- Re: Knowing probability just doesn't make a difference... (Henry Spencer)
- Reach Out and Spy on Someone (Pete McVay, Douglas Jones, Emily Lonsford)
- New Sprint Card (Will Martin)
- US missile-warning radar endangers friendly aircraft (Ken Arnold)
- Error free code and ancient systems (Bill Francis)

#### Issue 34 (2 Mar 89)

- German hackers breaking into LOS ALAMOS, NASA,...(Claus Kalle via Mabry Tyson)
- The Gumbel Machine Becomes a Candid Camera (PGN)
- (Un)fairness in European s/w protection (Herman J. Woltring)

# Issue 35 (6 Mar 89)

- NASA to replace top-level personnel with Expert Systems (Dave Davis)
- A Touching Faith in Technology (Ruaridh Macdonald)
- Computer catches thief (Randall [!] Davis)
- Computer espionage: 3 'Wily Hackers' arrested (Klaus Brunnstein)
- Re: West German Hackers (Dana Kiehl)
- The word "hacking" (Geoffrey Knauth, Rao V. Akella)
- 747 Simulators Can't Simulate Flight 811 Failures (Scot E Wilcoxon)
- Viruses in the comics (Peter Merel, Tom Parker, Len Levine, Guy Robinson)

# Issue 36 (7 Mar 89)

- Malicious Hacking (Gene Spafford)
- News from the KGB/Wily Hackers (Klaus Brunnstein)

The fight to purify the word "hacker" is lost (Steve Bellovin, Brad Templeton)

- Dangers of Spy programs (John ffitch)
- Re: reach out and spy on someone (Vandenberg)
- Social effects of viruses (Don Alvarez)
- Previous message to RISKS misunderstood (John Sinteur) [Power failure problems]

#### Issue 37 (11 Mar 89)

- Computer blunders blamed for massive student loan losses (Rodney Hoffman)
- Prisoner access to confidential drivers' records (Rodney Hoffman)
- Ethics Question (Randall Neff)
- Risk of congenial machinery (Robert Steven Glickstein)
- · Limitless ATM's (Geoff Kuenning)
- Re: Faking internet mail (Stephen Wolff)
- Virus detector goes wrong (Dave Horsfall)
- Re: News from the KGB/Wily Hackers (Hans Huebner = `pengo')
- UK archive service [for European RISKS readers] (Dave Ferbrache)

#### Issue 38 (15 Mar 89 )

- Water Bug Computerization Messing Up Yacht Race (Robert Horvitz)
- Sunspots & Communications (Cliff Stoll, PGN)
- pengo and the Wily hackers (Klaus Brunnstein)
- Toshiba DOS 3.3 Backup deletes files (Fiona M Williams)
- Star Trek computer virus (Kevin Rushforth)
- Re: NASA to replace top-level personnel with Expert Systems (Henry Spencer)
- Pushbutton Banking (Lynn R Grant)
- Risks of telephone access to your bank account (Michael McClary)
- Limitless ATMs (John Murray)
- Re: Prisoner access to confidential drivers' records (Scot E Wilcoxon)
- Risks of Human Emulating Machinery (Jon Loux)
- New Sprint Card (Ken Harrenstien)
- Incoming-call identification (David Albert)

#### Issue 39 (16 Mar 89)

- Solar flares vs. garage door openers (Steve Bellovin, Peter Scott)
- Sunspots and Power Lines (John Coughlin)
- Man-machine interfaces and perception-impaired people (David A. Honig)
- Re: reverse engineering of type fonts (Herman J. Woltring)
- Re: Ethics Question (Marc Mengel)
- Re: Toshiba DOS 3.3 Backup deletes files (Jay Elinsky)
- Re: IBM's claims to omnipotence (Dr Robert Frederking)
- · Re: Pushbutton Banking (Tom Coradeschi)

## Issue 40 (17 Mar 89)

- Re: Sunspots & Communications (Jordan Brown, Gasbarro)
- Ethics of Copying Fonts (Jerry Schwarz)
- Policy Statement Request (Dave Grisham)
- Re: Incoming-call identification (Brint Cooper)
- Risks of telephone access to your bank account (Brint Cooper)
- Limitless ATMs (Emily H. Lonsford)
- Re: A Touching Faith in Technology (Henry Spencer)
- Risks of helpfulness (Henry Spencer)
- Work monitoring survey (Goun)

- Faking Internet mail (Robert C. Lehman)
- Spying on or intercepting UUCP mail (David Sherman)
- Hackers, cartoons, and computers (Doug Claar)

#### Issue 41 (20 Mar 89)

- 20+ year, \$100+ million Army software project (Jon Jacky)
- Formal methods to be applied in Australian railroad switching (Jon Jacky)
- Error in updating new specifications for call-routing (Pertti Jarvinen)
- Risks of Registering Shareware (A. Lester Buck)
- Risks of helpfulness (Jerome H Saltzer)
- Remote Smart-Cards (Ian W Moor)
- Re: so-called multi-gigabuck theft of information (Mark Brader)
- Re: NASA to replace top-level personnel with Expert Systems (Robert English)
- Meter Readers an Endangered Species? (David K. Black)
- Security of Electronic Mail (Karl Lehenbauer)
- Star Trek computer virus (Colin P.)

#### Issue 42 (20 Mar 89)

Automatic Caller Identification (Phil R. Karn, Robert Goldman, John Murray, Bernie Cosell, Karl Lehenbauer,
 Dean Riddlebarger, Mark Mandel, Phil R. Karn again, Benjamin Ellsworth, more or less chronologically)

#### Issue 43 (21 Mar 89)

- Outdated codes made US missiles useless (Henry Cox)
- Risks of dying batteries (Henry Cox)
- Things to do with a computer... (Joe Morris)
- Possible Cancer Risks from Cellular Phones? (Mike Trout)
- Supreme Court and Copyrights (ark)
- Mitnick plea bargain (Rodney Hoffman)
- Re: Risks of telephone access to your bank account (Phil R. Karn)
- Internet Security Plans (Vin McLellan)
- Duplicates due to network lossage? (\*Hobbit\*)

#### Issue 44 (21 Mar 89)

- Computer-Justified Citations (Kevin Driscoll)
- Vehicle ID tags, cont'd (Steve Smaha)
- Ethics question re fonts (Michael Harrison, Elliott S Frank)
- Risks of shirt-pocket size floppy disks (Roy Smith)
- Re: Pushbutton Banking (Robert English)
- Credit card magstripe-encoded pictures (Peter Scott)
- Re: Remote Smart-Cards, English and Welsh soccer (Craig Cockburn, Dick King)
- Re: Risks of Registering Software (Bill Murray)
- Collecting for Shareware (Bill Murray)

# Issue 45 (25 Mar 89)

- Wells Fargo Deposits Slip (PGN)
- Hospital Viruses (Dennis Steinauer and Joe Morris)
- Optical Scanning of Handwritten Purchase Orders (Hiram Clawson)
- Credit card magstripe-encoded pictures (Mike Trout)
- Cellular phones and health (anonymous, Dale Worley, R. Scott Truesdell)
- New method (risk) of demagnetizing floppies (Douglas B. Robinson)
- Microwave ovens (Don Chiasson)

#### Corrections to Internet Security Plans (David M. Balenson)

# Issue 46 (29 Mar 89)

- B-1B wept-swing swept-wing (PGN)
- Soviets Lose 2nd Mars Probe (PGN)
- Satellite failure due to unremoved lens Cap (PGN)
- Technology strikes again -- Dodge Spirits and Dodge Fever (Matt Fichtenbaum)
- Suing over runaway computer systems (Rodney Hoffman)
- Virus Hits Hospital Computers (Rodney Hoffman)
- Prank Virus Warning Message (Bruce N. Baker)
- Subversive bulletin boards (Eric Percival)
- UK Computer Threat Research Association (David J. Ferbrache)
- Will the Hubble Space Telescope Compute? (Paul Eggert)
- The Airbus disaster and Ada (Ted Holden via Bob Burch via jpff)
- DIAC-90 -- Call for Papers (Douglas Schuler)

# Issue 47 (1 Apr 89)

- Summary of recent news briefs on "hacker" activity (Anonymous)
- "Free Fall" -- new book on 1983 Air Canada near-disaster (Rich Wales)
- Farm worker killed by conveyor (Walter Roberson)
- Hackers dictionary in Japanese? (Les Earnest)
- Undetected Monitoring Programs and Privacy Rights (Donald B. Wechsler)
- Re: Ada and Airbus (John Knight via A. Blakemore and Mike Linnig)
- Galactic Hacker Party (Rop Gonggrijp)
- Virus in PKARC software (Bob Kozlarek via Robert Casey via A-N-Onymouse)
- Computer Documentation Course Queries (Stephen W. Thompson)

#### Issue 48 (3 Apr 89)

- BMW's DWS system (Brian Randell)
- Risks of insomnia (Roger H. Goun)
- VDT Risks? No. Lead pipe cinch. (F. Baube)
- Aircraft running out of fuel in flight (Dale Worley)
- Yet another round of Airbus A320 discussions (Joe Morris)
- Daylight savings change requires computer shutdown (Walter Roberson)
- Elevator accident kills 13 year old (Walter Roberson)
- Re: "Free Fall" -- new book on 1983 Air Canada near-disaster (Henry Spencer)
- Newspapers' computer access to public records (Wm Randolph Franklin)
- Computers and Property Revaluation: It's Great in Dayton, Ohio (John Karabaic)
- Credit card magstripe-encoded pictures (Brian Randell)
- Using Pre-release Software (David A. Honig)
- Computer say, go to jail (Clifford Johnson)
- Accidental erasure of magnetic media used by the public (Peter Jones)

#### Issue 49 (5 Apr 89)

- An unusual "common mode failure" in B-1B aircraft (PGN)
- Gripen crash caused by flight control software (Mitchell Charity, Mike Nutley)
- Airbus A320 article plus some comments (Nancy Leveson) [long]

# Issue 50 (5 Apr 89)

- Mechanical Horse Racing (Mike Trout)
- Elevator death update (Walter Roberson)

Re: Elevator accident kills 13-year-old (Eric Roskos)

- Federal Pay System botch-up (Tim Shimeall)
- NYTimes business readers shown the future (Mitchell Charity)
- Newspapers and access to public records (J. Eric Townsend)
- High-Tech Locomotives (Mark Brader)
- Military software (Henry Spencer)
- Authenticating Internet mail (Peter Scott)
- Advertising vs the net (Brian Kantor via Skip Montanaro)
- Gorillas in the Missed Identification (Joe Morris, Jay Elinsky, Eddie Caplan)

# Issue 51 (6 Apr 89)

- Valdez Autopilot (Glenn Lea)
- The National Weather Service automation vs. aviation (Randal L. Schwartz)
- · Authenticating Internet mail (Jon Rochlis)
- Mechanical horse racing (Brad Hutchings)
- Re: Airbus A320 article (Dan Swinehart, Robert Dorsett, PGN)
- More on 1983 Air Canada near-disaster (Rich Wales)
- ATM loss no one believes the customer. (jrl)
- BMW Risks (Peter Kendell)
- BMW Road Warmers (Dennis Vadura)

# Issue 52 (9 Apr 89)

- Valdez follow-up... (Dean Riddlebarger)
- Phobos (Bob Morris)
- Presumption of innocence -- for computers (Peter da Silva)
- 1988 Toronto election (Mark Brader)
- · California's anti-fax-ad bill (David M. Gursky)
- Man bytes dog (Charles Youman )
- Re: Elevator accident kills 13-year-old (John Luce via John (J.G.) Mainwaring)
- Need DRAMs? (Mike Raffety)
- Cellular telephones (Steven C. Den Beste)
- CDC operating system has passwords in batch files (Gerard Stafleu)
- Cornell Chronicle coverage of Robert T. Morris (Manny Farber via Dave Farber)

#### Issue 53 (10 Apr 89)

- Product Recalls Due to Software Error (B.J. Herbison) [Medical]
- Airliners running out of fuel in mid-flight (Jerome H. Saltzer)
- Good press in Flying (Howard Gayle)
- Re: More on 1983 Air Canada near-disaster (Henry Spencer)
- PC causes multiuser host to drop off the network (Patrick Wolfe)
- Auto Risks (Robert Dorsett)
- Risk of Living in Nova Scotia (Matthew Wall)
- Otis elevator software (Eric Roskos)
- Elevator Units (Don Alvarez)
- Nuclear-powered vessels (Steve Bellovin)
- (Deep-seated) Presumption of innocence -- for computers (ephraim)
- Re: Authenticating Internet mail (John Labovitz)
- Passwords in plaintext (Brian McMahon)
- Re: Cellular telephones (Eric Thayer, David Collier-Brown)

#### Issue 54 (11 Apr 89)

• More on Otis 401 elevators (Dave Horsfall)

- PC crashing network: blame the error message (Mark Mandel)
- Election tampering and illegal surveillance (Brad Sherman)
- Computer CAN attempt to defraud you (Peter van der Linden)
- Infallible Computers (Dave Curry)
- Re: Airliners running out of fuel in mid-flight (Alan Marcum)
- Re: More on 1983 Air Canada near-disaster (Alan Marcum)
- Airbus A320 article plus some comments (Greg Rose)
- Re: CDC operating system has passwords in batch files (Steve Lidie)
- NSA and Not Secure Agencies (Curtis Spangler)
- California's anti-fax-ad bill... (Mark Mandel)

#### Issue 55 (12 Apr 89)

- Informing the Public about Risks (Marc Rotenberg)
- Central Locking Systems (J M Hicks)
- Social Security Administration Verifying SSNs (David Gast)
- Not Secure Agencies (Hugh Miller)
- Re: Cellular Telephones (Eric Roskos)
- Risk to Sun 386i users (Mike O'Connor via Alan Wexelblat)
- Infallible Computers and Perry Mason (Brinton Cooper, Ephraim Vishniac)
- Air Canada and fuel-proof gauges (Robert Dorsett, John Hascall)

# Issue 56 (13 Apr 89)

- Student grants debited instead of credited (John Harper)
- Electronic Truant Officers (Mike McNally)
- "Virus" arrest in New Jersey (A. Michael Berman)
- H.D. Thoreau on Risks of Believing Computations (David A Honig)
- Knowledge and Power (David Guaspari)
- "Malicious" computers? (Clifford Johnson)
- Re: Infallible Computers and Mason (Jack Holleran)
- HP MPE V/E Batch Security (Brown)
- More on the Sun 386i security hole (David C. Kovar via Alan Wexelblat)

#### Issue 57 (15 Apr 89)

- H.D. Thoreau on Risks of Believing Computations (Jim Haynes)
- Airbus 320 (Brian Randell)
- 1,000 Pilots Face ban (Dermot Williams)
- RFI and elevators (Robert A. Morris)
- Electronic Truant Officers (Carolyn M. Kotlas, Michael R. Hoffman, Ed Robertson)
- Re: Computer CAN attempt to defraud you (Hugh Davies)
- Computer maliciousness (Peter da Silva)

## Issue 58 (17 Apr 89)

- Cruise Missiles with "Polish" (Ralph Vartabedian via Nancy Leveson)
- Computerized parts supply (Jim Haynes)
- RFI and Elevators (Martin Ewing)
- Aegis the almighty (Henry Spencer)
- Thoreau and Navigation (Eric Roskos)
- Risks of automatic order entry in restaurants (Daniel Klein)
- Re: Most Accurate Clock (Clay Jackson)
- Fuel Management/Mis-management (Mike Brown)
- Companies mask ANI to calm callers (Bob Wallace via GEBM)
- The dangers of electric windows (Martin Cooper)

Careless tape transfer procedures (Peter Jones)

# Issue 59 (18 Apr 89)

- More on the British Midlands 737 crash (Robert Dorsett)
- Computers and Food Poisoning [anonymous]
- The dangers of electric seatbelts (was: windows) (Clements)
- Re: The dangers of electric windows (Daniel Klein)
- Newspaper Cartoons and Computer Infallibility (G. McClelland)
- Re: Thoreau and Navigation (David A Honig)
- "Journalist Vigilantes" (Walter Roberson)
- Hazards of RF near electronic controls (Dana Myers)

#### Issue 60 (19 Apr 89)

- Hillsborough: Risks of using Computers at Stadium Turnstiles (Brian Tompsett)
- Risks of plaintext data (Hugh Miller)
- Computer voting at Stanford (Scott Seligman)
- Re: Computerized attendance (Sean Fagan)
- More Auto-Seatbelt Horrors (Thor Simon)
- Mb = 1024? 1000? (Walter Roberson)
- Re: Newspaper Cartoons and Computer Infallibility (Will Martin)

#### Issue 61 (20 Apr 89)

- Alleged Computer-aided fraud (Rodney Hoffman)
- Black box for automobiles (Anthony Stone)
- References to smoking and computer failure? (David A Rasmussen)
- The danger of testing (re RFI and elevators) (Dave Collier-Brown)
- Reaction to John Luce's letter on electronic elevators (Peter Jones)
- Industry not protecting privacy (Rodney Hoffman)
- Sun386i security problem update (Ed DeHart)
- Writing on "write-protected" disks (David M. Zielke and Peter Jones)

#### Issue 62 (24 Apr 89)

- Release SkyDome, Release 0.0 (Mark Brader)
- Risks of plaintext data (II) (Hugh Miller)
- Computer orders for phone books (Mark Brader)
- ATM's used to track accused killer (Al Stangenberger)
- Computer Voting (Chris Davis)
- Re: Most Accurate Clock (David Schachter)
- Writing on write-protected disks (Leigh L. Klotz, Kenneth R. van Wyk, Phil Goetz, Dimitri Vulis, Henry Spencer, Dave Kemp, Rich Sims)

## Issue 63 (25 Apr 89)

- More 737 Computer Problems (Brian Randell)
- Cockpit Computers Defy Pilots (Robert Dorsett)
- Common thread in recent postings: People (Ian)
- Smoke vs. disc drives (John Shipman)
- Use of "Standard" on sensitive applications (Terry S. Arnold)
- Computer Threat Research Association (UK) (David J. Ferbrache)
- ATMs used to track accused killer (Steve Bellovin)
- Re: Most Accurate Clock (Don Watrous)
- Issue 64 (26 Apr 89)

- DARPA studying high-tech surveillance for drug wars (Jon Jacky)
- Re: SKYDOME (Michael Wagner)
- Cursing the Darkness? (Ronald J Bottomly)
- Data Checking at Osco's (Scott Turner)
- Re: Common thread in recent postings: People (Hugh Miller, John Karabaic)
- Re: Use of "Standard" ... (Pete Schilling, Steve Bellovin)

#### Issue 65 (27 Apr 89)

- Northwest 255 -- Another Disconnected Alarm story? (Jerry Leichter)
- All addressed up with the wrong place to go (Jerry Leichter)
- Jukebox foolishness (Robert J. Reschly Jr.)
- Electronic Seat-Belts (Marc W. Mengel)
- Mitnick plea bargain rejected by judge as too lenient (Rodney Hoffman)
- Spider-Man's SSN and computer limitations (Brad Blumenthal)

#### Issue 66 (4 May 89)

- Standards == nothing (Rich Neitzel)
- Traffic Alert Collision Avoidance System with "no bugs" (Henry Schaffer)
- Nuclear reactor knocked offline by 2-way radio in control room (Wm. Randolph Franklin)
- B-2 builders: Prototype not needed (Long Article) (Mark Thompson via Stephen W. Thompson)
- American Express is watching... (Sundar Iyengar)
- Telephone line security (David C. Kovar)
- COMPASS Program (John Cherniavsky)

#### Issue 67 (7 May 89)

- Space software problems (Henry Edward Hardy) [Magellan, Phobos I]
- Self-diagnostics in airplanes (David Robinson)
- B-2 Builders: Prototype not needed (Dave Parnas, Bill Murray, Henry Spencer)
- Standards == Nothing (Dave Parnas, Bob Estell, Henry Spencer)
- Risks to contact lenses wearers from computer ventilators (Periklis Tsahageas)
- Re: Telephone line physical security (William M. Bumgarner, Mike Akre)
- Power lines and computers (George Michaelson)
- Not using computer helps trapping of error (Konrad Neuwirth)

# Issue 68 (8 May 89)

- Low-Probability / High-Consequence Accidents -- and the Midland 737? (PGN)
- "Probing Boeing's crossed Connections" (Werner Uhrig)
- An Atlantis spacecraft computer problem resolved nicely (PGN)
- "Life's Risks: Balancing Fear Against Reality of Statistics" (Marc Rotenberg, Jerry Leichter).
- Hear No Evil (Kevin Driscoll)
- Computer Ethics Course/Resource Volunteers Wanted (long) (Bob Barger)

#### Issue 69 (10 May 89)

- Computers and Redistricting (PGN)
- Re: Atlantis spacecraft computer problem resolved nicely (Henry Spencer)
- Computer-generated checks (Art Werschulz)
- Re: Hear No Evil (Clay Jackson)
- Computer Bugs/Recalls/Upgrades (Clay Jackson)

#### Issue 70 (12 May 89)

- Computers in mathematical proofs (Henry Spencer)
- Re: An Atlantis spacecraft computer problem resolved nicely (Yves Deswarte)
- Company sued for "computerized" firing scheme (Emily H. Lonsford)
- Logged on and Unattended (NOT FROM Jon Orseck)
- Dot Matrix == valid and LaserReceipts (Mike Albaugh)
- Computer generated checks (John McLachlan, Darin McGrew)
- Auto electronics and Radio Transmitters don't mix! (Peter Morgan Lucas)
- Mitnick update (Rodney Hoffman)
- TRW & SSA (Michael J. Tighe)
- Centralized Railroad Dispatching (Chuck Weinstock)

#### Issue 71 (17 May 89)

- American Airlines' reservation system crash (Dave Curry)
- NCIC information leads to repeat false arrest suit (Rodney Hoffman)
- Hacking for a competitive edge (Rodney Hoffman)
- Privacy of SSA records (Marc Rotenberg)

#### Issue 72 (21 May 89)

- Air Force Bombs Georgia (henry cox)
- The Geomagnetic Storm of 13 March 1989 (Brian Randell)
- Tolerability of Risk (Martyn Thomas)
- More magnetic stripe woes (Joe Morris)
- Dive Computers revisited (Henry Cox)

# Issue 73 (22 May 89)

- State computer system scrapped (Bruce Forstall)
- Fax Attack (Chuck Dunlop)
- Client responsibility for organization's head crash (David A Honig)
- Re: Computers in mathematical proofs (Robert Lee Wilson Jr, Robert English, Travis Lee Winfrey)
- Formal Methods -- Call For Papers (Nancy Leveson)

#### Issue 74 (26 May 89)

- Aegis, Vincennes, and the Iranian Airbus (PGN interpreting Matt Jaffe)
- Anti-lock brake system failure fail-safe? (Jay Elinsky)
- Pleasure boat database helps thieves (Howard Gayle)
- SAGE-BOMARC risks (Les Earnest)
- SABRE disaster caused by "core corruption" (Andrew Birner)
- Computer Intrusion Network in Detroit (Dave Curry)
- Robert T. Morris suspended from Cornell (Dave Curry)

## Issue 75 (30 May 89)

- Mariner I -- no holds BARred (PGN)
- Another false incarceration (PGN)
- Perfecting Peopleware (Bob Morris)
- Aegis and the Iranian Airbus shootdown (Steve Philipson)
- Radio Frequency interference (J. Michael Berkley)
- SRI attacked by kamikaze squirrels? (David L. Edwards)
- Computer electrocutes chess player who beat it! (Gene Spafford)

## Issue 76 (31 May 89)

• State computer system scrapped (Davis)

- Swedish library loan data to become secret (Howard Gayle)
- SABRE (Bill Murray)
- Strange Customs Service Clock Department (Willis H. Ware)
- No power lunch, just no-power crunch (after the squirrel's over) (PGN)
- Re: Computer electrocutes chess player who beat it! (David Chase)
- Five admit automated teller scam (Rodney Hoffman)
- Re: Kevin Mitnick (Kenneth Siani)

#### Issue 77 (8 Jun 89)

- Second elevator death (Walter Roberson)
- Electronic card spots hooligans (Martyn Thomas)
- Big Brother is watching your magnetic card (Amos Shapir)
- May you live in interesting times (High-tech Chinese revolution)(Martin Minow)
- "Core-Walker" that crashed SABRE (Rodney Hoffman)
- Airbus A320 (Brian Randell)
- Re: Power outages (Peter Scott)
- One of Cliff Stoll's 'Wily Hacker' dead (suicide?) (Klaus Brunnstein)
- Computer Virus Catalogue (Aims and Scope) (Klaus Brunnstein)

### Issue 78 (11 Jun 89)

- NY Telephone Freebies (PGN)
- Nielsen Raidings -- A risk? (John Rushby)
- C-17 Overrun (Gary Chapman)
- COMPASS '89 reminder (Al Friend)
- Re: Big Brother is watching your posting in RISKS (Amos Shapir)
- How Rumors Mutate, Lesson 2 (Rich Fritzson)
- The computer didn't commit the crime (Michael Doob)
- An ATM gets it right (Steve Anthony)
- Justice Department wary in Computer Case (Dave Bozak)

## Issue 79 (14 Jun 89)

- Single point of failure -- Tokyo Stock Exchange (Jerry Carlin)
- Costly Horse Race (Rick Zaccone)
- Commercial Loans in California at a Standstill (PGN)
- Phone Hacking (Brinton Cooper)
- Microcomputers in the operating theatre (Martyn Thomas)
- Inspiration from the past -- Machines Will Take Over (Curtis Galloway)
- "Illuminatus!" (Pete)
- Praise and Blame -- Computers and People (Hugh Miller)
- NORAD Computers: Years Late, Unusably Slow, \$207 Million Over Budget (Karl Lehenbauer)

#### Issue 80 (16 Jun 89)

- Disarmament by defect (Gerard Stafleu)
- Even human-in-the-loop isn't foolproof. A test case. (Pete Holzmann)
- Single point of failure? probably not. (Ephraim Vishniac)
- Re: single point of failure -- Tokyo Stock Exchange (Patrick Wolfe)
- Qantas Airliner Mishap (John Murray)
- Theorem Proving by Computers (Tom Thomson)
- Re: Computer electrocutes chess player ... (Dave Horsfall, Joel Kirsh)
- Clerical error spares famed sex-fiend (Mike Albaugh)
- Sabre computer problems revisited (Emily H. Lonsford)
- Protection from Misdirected Radio Control Commands (Robert Horvitz)

#### Issue 81 (17 Jun 89)

- Re: Disarmament by defect (Gary Chapman)
- Medical history-on-a-card? (Ellen Keyne Seebacher)
- No backups -- TOWER of Babel (Sam Cramer)
- 'Blip' Blows Computers Back to Paper Age (Mark Osbourne)
- Re: Computer electrocutes chess player who beat it! (O. Crepin-Leblond)
- Re: Hartford Coliseum (Richard S. D'Ippolito)

### Issue 82 (19 Jun 89)

- Re: Microcomputers in the operating theatre (Ken Howard)
- Risks of missiles (Steve Den Beste)
- Trojan Horse in Comp.Risks? (John C Williams)
- Power glitches scrambling computers --- can it be avoided? (Will Dickson)
- Re: 'Blip' Blows Computers Back to Paper Age (William M. Bumgarner)
- No back-ups: Ninth Circuit's "computer error" (Clifford Johnson)
- Hillsborough Football -- Another Computer Connection (Charles Lindsey)
- Radio Control Interference (Marco C. Barbarisi)
- New Yorker Article (book serialization?) on radiation risks (Martin Minow)

#### Issue 83 (20 Jun 89 PDT)

- Pacemakers, radios (Walter Roberson)
- 'Traffic monitoring system used for spying' (Walter Roberson)
- I am not a number... (unique postal codes) (Walter Roberson)
- Medical history-on-a-card?; Another ATM Risks (Edward A. Ranzenbach)
- Re: Microcomputers in the operating theatre (Donald Lindsay, Keith Emanuel)
- Hartford Civic Center roof crash (Peter Desnoyers)
- Re: Risks of missiles (Jan Wolitzky, Gary Chapman, Bob Ayers)

#### Issue 84 (21 Jun 89)

- The risks of global editing (Martyn Thomas / Richard Tobin / Nick Radcliffe)
- Re: I am not a number -- already in the US (Tom Comeau)
- Re: I am not a number -- more in Canada (Vince Manis))
- Re: Computer electrocutes chess player ... (W. Scott Meeks, Brendan McKay)
- Gigatext Translation Services Inc. scandal (Bhota San) [long]

#### Issue 85 (28 Jun 89)

- Air Force satellite positioning system cracked (Dave Curry)
- Loose wire caused Clapham train crash (Jon Jacky)
- London firms reportedly offer amnesty to "hacker thieves" (Ken Berkun via Jon Jacky)
- Re: Microcomputers in the operating theater (Jon Jacky, Diomidis Spinellis)
- Don't celebrate big tax refund too quickly (David Sherman)
- Reading meters and gauges by robot in nuclear power plants (Robert Cooper)

# Issue 86 (29 Jun 89)

- SPADOC Modernization Effort (Chris McDonald)
- Are are nuclear weapons useable? How can one test this? (Dennis L. Mumaugh)
- NASA tests video system that may lead to windowless cockpits (Karl Lehenbauer)
- Air Force to upgrade missile launch command computers (Jon Jacky)
- Missile launch -- upgrades degrade ? (Clifford Johnson)
- Strategic weapon software development practices (Stan Shebs via Jon Jacky)

- Rotting Landsat data (Jonathan Patrick Leech)
- Issue 87 (29 Jun 89)
  - "Student plan marred by computer mistake" (Matthew Wall)
  - Immigration Chief Proposes National Computer Screen (Christopher T. Jewell)
  - Big Brother is Hallucinating (Elizabeth D Zwicky)
  - Study finds "pedal misapplication" to blame for Audi surges (Jon Jacky)
  - Computer Crime and Social Risks (Pete McVay)
  - Reducing risks of cost overruns/project failures (Pete Lucas)
  - Re: New Yorker Article on radiation risks (David Chase)
  - Computerized Translations (Will Martin)



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 8: Issue 1

# Wednesday 4 January 1989

# **Contents**

- Tales from the Vincennes tape
  - **Rodney Hoffman**
- A Danish Home Companion
  - **Hugh Miller**
- Suit filed to force FBI to enforce privacy provisions of ECPA John Gilmore
- moRe: Armed with a keyboard ... -- Kevin Mitnick Rodnev Hoffman
- Computer Chaos Congress 88 report
  - Klaus Brunnstein
- Two steps forward, one step back
  - Jerry Leichter
- Clapham Junction train crash Clive Feather via Mark Brader
- Info on RISKS (comp.risks)

# Tales from the Vincennes tape

Rodney Hoffman <Hoffman.ElSegundo@Xerox.com> 28 Dec 88 08:27:03 PST (Wednesday)

Congressman Les Aspin (D - Wis.) is the chairman of the House Armed Services Committee. In an op-ed piece in the 28 Dec 88 'Los Angeles Times,' he writes about the rarity of naval combat and about needed improvements in the Navy's training, screening, and scheduling. To make his case, he tells details from the Vincennes' shootdown of an Iranian commercial jet last July:

The crew was green when the battle began. And it showed. Despite all the training that the crew of the Vincennes received, the reality of battle was something new and nerve-racking. We can tell how nerve-racking it was from the unique electronic record kept by the Aegis system aboard the Vincennes. It recorded such details as the precise moment in which every button was touched and every toggle switched in the Vincennes' command center.

Because of this record, we know that one officer, who was prompted by the computer to "select weapon system" as the countdown to the destruction of the Airbus began, hit the wrong buttons five times before he realized that he was supposed to select a weapon. And we also know that another member of the Vincennes' crew was so agitated that he got ahead of the firing sequence and pushed another button 23 times before it was an appropriate part of the procedure.

I don't recount these errors to pick on the crew. I recount them because I believe that they much be considered the norm when inexperienced humans face a sudden stressful encounter.....

# A Danish Home Companion

<Hugh Miller <MILLER@vm.epas.utoronto.ca> [MILLER@UTOREPAS.BITNET]>
Mon, 02 Jan 89 22:47:40 EST

I found the following quote in the journal of Soren Kierkegaard for 1850. As this is the time of year we traditionally form our resolutions for the next, I thought it might be helpful for us on the RISKS list to bung this into the hopper for consideration. The really good ideas never die; they just change examples.

"It is the old story. A discovery is made--the human race triumphs; enthusiastically everything, everything is set going to perfect the discovery more and more. The human race is jubilant and worships itself. At long last there comes a halt--man pauses and asks: is this discovery really a boon, especially the extraordinary perfection of it that has been achieved! Then a new call goes out for the most eminent heads, and they torture their brains almost to madness to find safety-valves, dampers, clogs, etc. in order, if possible, to put a brake on, to prevent this matchless and matchlessly perfected discovery, the pride of the human race, from riding roughshod over the whole world and destroying it. Consider, for instance, the invention of the printing press, perfected to a top-speed machine sure to guarantee that no dirt or dregs remain unpublished."

A Happy and Safe 1989 to everyone! Hugh Miller University of Toronto

## Suit filed to force FBI to enforce privacy provisions of ECPA

John Gilmore <gnu@toad.com> Thu, 22 Dec 88 18:29:47 PST

In January 1988, Riverside, CA coroner's deputies obtained a warrant to seize all the computers at the Alcor Life Extension Foundation. This was done in connection with the widely reported cryonic suspension of 83-year-old Dora Kent. The coroner accused the Alcor staff of murder, arguing that the cryonics procedure, where life support and anesthesia/cooling is applied after legal death, is murder, because resuscitation technology is applied without the intent

to revive the patient.

The deputies took six or seven computers ranging from an Apple II to an Amiga, and have held them for the last 11 months.

Only one of these had a hard disk, so there wasn't much they could get out of the computers anyway. However, they did succeed in making it much more difficult for Alcor to conduct business.

The computer with the hard disk was being used as a bulletin board. Some 50 to 100 people had correspondence on the machine. No warrants, not even any "John Doe" warrants, were issued which would permit the coroners, DAs, or the Riverside Police Department to access these electronic communications in storage under the Electronic Communications Privacy Act. The ECPA requires that the particular people whose communication is to be seized be named in the warrant, similar to the warrants required to seize a person's postal mail. This search warrant specified that "all electronic storage devices... and the complete hardware necessary to retrieve electronic data" be confiscated, not even naming Alcor, but simply giving the address of their office.

Keith Henson (best known for founding the L5 Society, which encourages the exploration of outer space) was one of the people whose email was confiscated. He complained to the FBI about his email being taken without a warrant last April. The FBI Riverside office inquired of the US Attorney's office as to their interest in email, and, on getting a "not interested," declined to investigate. Henson tried through his congressional representatives to get enforcement action out of the Federal government against the various local law enforcement agencies who had taken his email.

Finally, becoming convinced that this route was ineffective, Henson and two other bbs users filed suit against the US Attorney's office and the FBI. One of the bbs users, Roger Gregory, is well known for guiding project Xanadu, the proposed hypertext library system; the other, Thomas Donaldson, has contributed two science fact articles to Analog magazine in the last year. The suit, "Complaint for Declaratory Judgement" number C 88 20788, was filed in the U.S. District Court for the Northern District of California on December 9, 1988.

The crux of the matter is whether the ECPA prevents electronic mail from being read if the entire computer containing the mail is seized under a warrant. If this is held true, the ECPA provides little or no actual protection. Consider the non-electronic or real-time analogies; can a warrant that names no names be used to seize and read all the mail in a building providing private post office boxes? Can a warrant claiming that someone is doing something illegal in a telephone company office be used to tap all the subscribers' lines going through that office?

A complete online copy of the suit (40 kbytes) is available as email from keith@toad.com. He can also send out hardcopies for the disabled,

or for people whose email has been seized. The plaintiffs are:

H. Keith Henson +1 408 978 7616 keith@toad.com
Thomas K. Donaldson +1 408 732 4234 cis 73647,1215; source beb610
Roger E. Gregory +1 415 493 7582 roger@xanadu.com

# moRe: Armed with a keyboard and considered dangerous

Rodney Hoffman <Hoffman.ElSegundo@Xerox.com> 28 Dec 88 14:39:59 PST (Wednesday)

A follow-up story to the Kevin Mitnick case [see <u>RISKS 7.95</u>] in the 'Los Angeles Times' 24 Dec 88 says the federal magistrate refused to release Mitnick on bail 23 Dec 88

after prosecutors revealed new evidence that Mitnick penetrated a National Security Agency computer and may have planted a false story on a financial news wire....

Investigators believe that Mitnick may have been the instigator of a false report released by a news service in April that Security Pacific National Bank lost \$400 million in the first quarter of 1988. The report, which was released to the NY Stock Exchange and other wire services, was distributed four days after Mitnick had been turned down for a job at Security Pacific [after the bank learned he had lied on a job application about his past criminal record].... The false information could have caused huge losses for the bank had it reached investors, but the hoax was uncovered before that could happen.

The prosecutor said Mitnick also penetrated a NSA computer and obtained telephone billing data for the agency and several of its employees....

[In refusing bail, the magistrate said,] "I don't think there's any conditions the court could set up based upon which the court would be convinced that the defendant would be anything other than a danger to the community.... It sounds like the defendant could commit major crimes no matter where he is."

Mitnick's attorney said prosecutors have no evidence for the new accusations....

# Computer Chaos Congress 88 report

Klaus Brunnstein <br/>
<br/>
Stein%rz.informatik.uni-hamburg.dbp.de@RELAY.CS.NET>
03 Jan 89 09:50 GMT+0100

Re: Observing Chaos Communication Congress 1988, Hamburg (`From Threat to Alternative Networks')

Date: January 2nd, 1989

On 28-30 December, 1988, Computer Chaos Club (CCC) held its 5th annual 'Chaos

Communication Congress' at Hamburg/FRG. As in previous years, 300 people (mainly aged 16-36, 90% male, with some visitors from Austria and The Netherlands) gathered, carefully observed from newsmedia (German stations, printmedia, press agencies, but also from UK's BBC, and being observed by Business Week's Katie Hafner, who gathered material for a book on hackers, planned by John Markoff and herself).

In the chaotic (though creative) congress 'organisation', two different tracks were visible:

- -- technical presentations on networks (UUCP, GEONET, FIDONet, and CCCs emerging `open networks' BTXnet and `Zerberus'), and on a PC-DES encryption developed by a leading CCC member (who had escaped the French police's arrest by travelling to SECURICOM by railway while police waited at the airport);
- -- socio-political discussions about `sociology of hackers',
   `free flow of information' as well as reports about
   recent events, dominated by the arrest of Steffen Wernery
   in Paris in spring 88 when being invited to speak on SECURICOM.

The technical presentations were of mixed quality. The PC-DES program (evidently written under the experience of several `visits' of German criminal police on search for convicting material in cases of hacker attacks) encrypts texts with a key of 8-40 characters, with a velocity of 135 characters/second (on a 10 MHz 80286 processor); in a demonstration, the stored `Congress report' of 137.416 Bytes was encrypted (without prior compression) in 2:55 minutes. The recent version (V.2.02: about 8 kByte long including about 4 kByte of help-text) was distributed at CCCongress as `Charity-ware' (for hackers free of charge), but will be available for commercial users from German `Security advisor' Hans Gliss at 250 DM (about 141 Dollars at actual exchange rates).

CCC speakers reported about their work to install 'free networks'. In Germany, most of the networks are organised in the form of a 'Verein' (an association with legal status, which guarantees tax-free operation): such networks are access-restricted to their members. The different German science and University networks (and their bridges to international networks) usually restrict access to scientists. Different CCC subgroups are establishing 'alternative networks', such as 'EcoNet' for communication of ecological data and information, planned to be available, free of cost, to broader social, ecological, peace and political groups and individuals.

Apart from traditional technologies (such as GEONET and FIDONet), the German Post Office's Bildschirmtext (Btx) will be used as a cheap communications medium; while CCCs first hack was, years ago, to attack the `insecure Btx-system' (in the so-called `HASPA coup' where they misused the Btx passwork of the Hamburg savings bank to repeatedly invoke CCC's Btx information at a total prize of 135.000 DM, then about 50.000\$), they today begin to use this cheap though very limited medium while more powerful communications media are available. Today, the emerging ISDN technology is verbally attacked by hackers because of the excessive accumulation of personal data; from here, hacks may be attempted when ISDN becomes regionally available in 1989/90.

Several speakers, educated Informaticians with grades from West German Informatics departments, professionally work in Software production and in selling hardware/software to economy and state agencies. Among them, several professional UNIX and UUCP users have begun to organize CCC's future UUCP version. Up to now, only few CCC members use (and know about) UNIX systems, but their number may grow within the near future according to CCCs `marketing'. One speaker told the audience `that you can remotely start programs in UUCP'. After some learning phase, the broadened availability of UNIX in the hacker scene may produce new threats.

The other track of the Congress discussed themes like 'sociology of hackers' where a group of politology students from Berlin's Free University analysed whether hackers belong to the 'new social movements' (e.g. groups on peace, nuclear energy, feminist themes). They found that, apart from much public exaggeration ('it is not true that hackers can invade \*any\* computer'), hackers are rather 'unpolitical' since they are preferably interested in technology.

A major topic was 'free access to/flow of information'. Under the title 'freedom of information act', speakers suggested a national legislation which guarantees individual and group rights to inspect files and registers of 'public interest'; the discussion lacked sufficient basic knowledge, e.g. of the respective US legislation and corresponding international discussions in Legal Informatics. Generally, the published results of the rich discussions about 'Social aspects of Computing', gathered in professional bodies (like ACMs SIGCAS, IFIPs TC-9 or the German national society's FA-8, all devoted to such themes) are evidently unknown to this scene.

Summarising the Congress and accompanying discussions, active CCC members try hard to demonstrate that they have \*no criminal goals\* and ambitions (they devoted a significant amount of energy to several press conferences, TV discussions etc). The conference was dominated by young computer professionals and students from the PC scene, partially with good technological knowledge of hardware, software and networks; while some people seem to have good technical insights in VAXsystems, knowledge of large systems seems to be minimal. To some extent, the young professionals wish to behave as the 'good old-fashioned hackers': without criminal energy, doing interesting work of good professional quality in networks and other new areas.

While former CCCongresses were devoted to threats like Viruses, \*no explicit discussion\* was devoted \*to emerging threats\*, e.g. in ISDN or the broadening use of UNIX, UUCP. The new track discussing political and social aspects of computing follows former discussions about `hacker ethics'. Here, the superficial, unprofessional discussions of related themes show that the young (mainly) males are basically children of a `screen era' (TV, PCs) and of an education which concentrates on the visible `image', rather than understanding what is behind it.

(A 140 KBytes electronic Congress news`paper' can be mailed, on demand, to people who are interested in details; the papers, of mixed quality, are mainly written in German)

Prof. Dr. Klaus Brunnstein, Faculty for Informatics, University of Hamburg, Schlueterstr.70, D 2000 Hamburg 13 Tel: (40) 4123-4158 / -4162 Secr.

# Two steps forward, one step back

LEICHTER-JERRY@CS.YALE.EDU <"Jerry Leichter> Tue, 3 Jan 89 15:52 EST

As we well know, technological changes can produce unanticipated side-effects. The Editorial attached below, from a recent New York Times, provides an interesting illustration of such an effect.

A day or two later, the Article attached below appeared in the Times. What side-effects will this little piece of technology have?

-- Jerry

**EDITORIAL** 

Personal XXXXX's

Not many years ago, there were three kinds of typing and each sent its own message. Letters from a genuine V.I.P. were written on an elegant electric typewriter, with a carbon ribbon that printed sharp black letters. Letters from lesser lights were written on manual machines, nicely arranged and errorfree, but distinguishable by the grainy impressions of a fabric ribbon. Then there were the personal letters, in which strikeovers and xxxxx's demonstrated the exclusivity of the correspondence.

Now the word processor has erased this typology of typewriting. The early home printers with their coarse san-serif characters are yielding to new machines, including laser-jet printers, that make the layman's letters look like the elegant V.I.P. correspondence of old.

That's probably progress, but it comes at a cost. There's no telling, anymore, whether such a letter is personal. Once, you could discern from the typographical errors whether the annual chatty holiday letter was meant just for you, or for the whole Christmas list. Not anymore, not when home computers can "personalize" a mass mailing by changing the salutation and a tell-tale fact or two and printing it up beautifully.

The tide of progress, in other words, sometimes flows backward. There's probably only one sure way now to write letters that are, and look, personal: by hand.

ARTICLE

High-Tech Junk Mail

After installing a facsimile machine, many offices soon discover a byproduct of this high-tech communications form --- junk fax mail. When a facsimile machine is left on, anyone with access to the machine's telephone number is free to send documents to the machine, just as anyone with access to a postal address can send mail there.

Now Digital Publications of Norcross, Ga., has come up with a program and a data base that can be used with a specially equipped personal computer to send press releases en masse by facsimile machine. Late at night, when telephone long-distance rates are lowest, the computer and its facsimile-machine circuit board will automatically dial telephone numbers all over the country, sending out press releases.

Executives of Digital Publications contend that after 11 P.M. their system can deliver a news release for 10 cents. They said that a news release sent through the mail costs about 80 cents. Mail rates keep going up, of course, and delivery can take two or three days, or longer.

The Digital Publications system data base has 5,000 names and addresses of newspapers, broadcast stations, trade magazines and writers. Also --- and this is crucial --- it has each outlet's fax number.

But the new technology must still overcome the same hurdle that confronts the old technology of sending an envelope through the mails --- getting the recipient to read the material.

# Clapham Junction train crash

Mark Brader <msb@sq.sq.com> Tue, 3 Jan 89 21:30:26 EST

Clive Feather, a former contributor to Risks currently off the net but "soon to be clive@isi.co.uk", has sent me some information about the train crash at Clapham Junction in London last month. I have posted a longer version to Usenet's rec.railroad, but here's the meat.

#### Clive writes:

- # The BR internal enquiry found that there were no faults in the
- # signalling equipment as such, but a member of the S&T [Signals and
- # Telecommunications] department had failed to correcly tie off a loose
- # cable end. This was making intermittent contact with a signalling
- # structure (i.e. earth) and this in turn caused the preceding
- # signals to continually vary in aspect. Presumably the driver ...
- # was only looking at the wrong moment.

#

- # There will not be a normal enquiry and report. Instead, there will be
- # a full judicial enquiry, something that up to now has only happened
- # twice -- Tay Bridge [1897] and Hixon [~1968].

#

# I expect the February Modern Railways [magazine] will be full of this.

Forwarded to Risks by Mark Brader, Toronto











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 8: Issue 2

# Wednesday 4 January 1989

# Contents

Christmas 1988 Decnet Worm -- Counteracted Cliff Stoll

Vincennes and the computer

Steve Philipson

**Clifford Johnson** 

Viruses and System Security (a story)

by Dave Platt

submitted to RISKS from rec.humor.funny by Jim Horning and Mark Brader

Stallman, Minsky and Drescher on the Internet Worm

via Martin Minow

- FAA Orders Computer Card Security Systems at 270 Airports **Henry Mensch**
- Info on RISKS (comp.risks)

## Christmas 1988 Decnet Worm -- Counteracted

Cliff Stoll <cliff%cfa204@harvard.harvard.edu> Tue, 27 Dec 88 13:44:27 EST

On December 22nd, someone started a virus/worm on the SPAN/Decnet network. It attacks only Vax/VMS computers, and only those which are connected to the SPAN/HEPNET/Decnet network. It cannot enter Unix systems or PC's.

This virus/worm is benign in that it does not erase information. The writer apparently wishes to embarrass system managers and network administrators.

Language purists will call it a worm: it does not modify any files, and copies itself from node to node.

Indications point to an origin in Germany.

I spent several hours creating bogus announcements to confuse and counteract the virus writer. I've mailed these to the PHSOLIDE collection point.

The virus writer has collected these announcements, and has no way to tell which announcements are valid, and which are phoney.

Technical details for Decnet/VMS people:

The worm enters through the Decnet Task object, and mails your system's announcement banner (sys\$announce) to Decnet node 20597::PHSOLIDE. (This node apparently is in France)

The worm generates a random node address and tries to copy itself onto that node. If this fails, it tries different random nodes until it finds one.

Once it finds a valid node, it tries to copy itself using the NETFAL account (through the Task object). If you don't have a valid Task object, it tries to log into account DECNET, with password DECNET.

Once it's in your system, it creates a list of all users on your node, and mails a message to each of them. This message is some blather about how Father Christmas has had a hard time getting "the terrible Rambo-Guns, Tanks and Space Ships up here at the Northpole." The message itself is written in a stilted, almost Germanic, style.

You can immunize your system by deleting the TASK 0 Decnet object, and by making certain that you've changed the Decnet password. In any case, the worm is timed to stop after December 24th. By the time you receive this message, the worm will have died.

Cliff Stoll, Harvard - Smithsonian Center for Astrophysics,
60 Garden Street, Cambridge, MA 02138 Cliff@cfa200.harvard.edu

# Vincennes and the computer

Steve Philipson <steve@aurora.arc.nasa.gov> Fri, 23 Dec 88 15:03:50 PST

In RISKS-FORUM Digest 7.94 "Clifford Johnson" <GA.CJJ@Forsythe.Stanford.EDU> [Vincennes: conclusively, a computer-related error] writes:

>I reflect that \*all\* the information that panicked the Vincennes crew and >captain came from the computers. The captain was not faulted [...] > The fault was found to lie largely with the computer's initial >classification of the flight as hostile, and the computers' subsequent unclear >albeit correct presentation of the ascent data. The actions taken to remedy >the deficiencies are improvements in the computer display/ human interface. >This is a a classic case of computer \*related\* error: unobvious and secondary >display of criticial data.

>What the Pentagon has has more or less overtly ruled is that its >most competent, trained, and alert officers cannot be blamed for >mistakenly reading and acting on deadly computer displays, >especially not in combat, i.e. when they're actually used.

In the case of Vincennes, the computer was definitely NOT the only nor the most significant source of information. The ship had been primed with intelligence reports of hostile intent, was engaged in battle, maneuvering radically, and taking fire. The crew could hear bullets and shrapnel hitting the ship. They had been briefed to expect attack including aerial attack, and had the memory of the Stark to remind them of the dangers inherent in their situation. They knew they were under surface attack. They were ready to believe that they were about to come under aerial attack as well.

A major conclusion of the report was that people under great stress do not function in the same manner as they do in lab conditions. It's easy for us to scour through the records in the comfort of our homes and offices and make judgements, but far more difficult to make them under severe time pressure, in physically disturbing conditions, under the threat of death.

This case illustrated that a correct presentation of data is not always sufficient to prevent error; it may be necessary to present the data correctly and in a form that is highly unlikely to be misinterpreted. It is not clear that we will ever be able to make systems that are immune from misinterpretation under such severe conditions.

There is always confusion in battle, and there always will be, no matter what we do with computer systems. The commander's first duty was to protect his ship. That is what he did, albeit from what turned out to be a non-combatant that could not have hurt him. To censure the crew of the Vincennes would undermine the ability of every man in uniform to take the necessary actions to protect himself and his country. The Pentagon brass affirmed with their decision that battle zones are places rife with confusion and danger, and that errors under those conditions are a fact of life.

We learn from this incident that battle zones are no place for innocents (a lesson that is intuitively obvious), and that we have much to learn about how to fight with systems based on men and machines.

[...]

# Vincennes and the computer

"Clifford Johnson" <GA.CJJ@Forsythe.Stanford.EDU> Tue, 27 Dec 88 16:19:08 PST

- > In the case of Vincennes, the computer was definitely NOT the only
- > nor the most significant source of information.

What I meant was that without the computer, there wouldn't have even been a decision to shoot. The computer-sensor's recognition of military signals from the take-off airfield triggered, according to rule, an initial misclassification as hostile until proven otherwise, and without the computers' tracking of the flight nobody could have believed that the flight was diving towards the ship. That the error was due to bad presentation of data was the Pentagon's conclusion, and why the incident is conclusively

computer-related error.

- > To censure the crew of the Vincennes would undermine the
- > ability of every man in uniform to take the necessary actions
- > to protect himself and his country.

We agree that the conduct of men in such circumstances is inherently an input-governed impulse. But your sentiment overlooks that military mission takes precedence over personal survival, and that protection of innocent life in the Gulf was the Vincennes' mission. Viewed in this light, the reliance placed on the computer-governed drills is unconvincingly justified.

[...]

# Viruses and System Security (a story) [by Dave Platt]

Jim Horning <horning@src.dec.com> 20 Dec 88 00:30:03 GMT

The following story was posted in news.sysadmin recently.

The more things change, the more they stay the same...

Back in the mid-1970s, several of the system support staff at Motorola (I believe it was) discovered a relatively simple way to crack system security on the Xerox CP-V timesharing system (or it may have been CP-V's predecessor UTS). Through a simple programming strategy, it was possible for a user program to trick the system into running a portion of the program in "master mode" (supervisor state), in which memory protection does not apply. The program could then poke a large value into its "privilege level" byte (normally write-protected) and could then proceed to bypass all levels of security within the file-management system, patch the system monitor, and do numerous other interesting things. In short, the barn door was wide open.

Motorola quite properly reported this problem to XEROX via an official "level 1 SIDR" (a bug report with a perceived urgency of "needs to be fixed yesterday"). Because the text of each SIDR was entered into a database that could be viewed by quite a number of people, Motorola followed the approved procedure: they simply reported the problem as "Security SIDR", and attached all of the necessary documentation, ways-to-reproduce, etc. separately.

Xerox apparently sat on the problem... they either didn't acknowledge the severity of the problem, or didn't assign the necessary operating-system-staff resources to develop and distribute an official patch.

Time passed (months, as I recall). The Motorola guys pestered their Xerox field-support rep, to no avail. Finally they decided to take Direct Action, to demonstrate to Xerox management just how easily the system could be cracked, and just how thoroughly the system security

systems could be subverted.

They dug around through the operating-system listings, and devised a thoroughly devilish set of patches. These patches were then incorporated into a pair of programs called Robin Hood and Friar Tuck. Robin Hood and Friar Tuck were designed to run as "ghost jobs" (daemons, in Unix terminology); they would use the existing loophole to subvert system security, install the necessary patches, and then keep an eye on one another's statuses in order to keep the system operator (in effect, the superuser) from aborting them.

So... one day, the system operator on the main CP-V software-development system in El Segundo was surprised by a number of unusual phenomena. These included the following (as I recall... it's been a while since I heard the story):

- Tape drives would rewind and dismount their tapes in the middle of a job.
- Disk drives would seek back&forth so rapidly that they'd attempt to walk across the floor.
- The card-punch output device would occasionally start up of itself and punch a "lace card" (every hole punched). These would usually jam in the punch.
- The console would print snide and insulting messages from Robin Hood to Friar Tuck, or vice versa.
- The Xerox card reader had two output stackers; it could be instructed to stack into A, stack into B, or stack into A unless a card was unreadable, in which case the bad card was placed into stacker B. One of the patches installed by the ghosts added some code to the card-reader driver... after reading a card, it would flip over to the opposite stacker. As a result, card decks would divide themselves in half when they were read, leaving the operator to recollate them manually.

I believe that there were some other effects produced, as well.

Naturally, the operator called in the operating-system developers. They found the bandit ghost jobs running, and X'ed them... and were once again surprised. When Robin Hood was X'ed, the following sequence of events took place:

!X id1

id1: Friar Tuck... I am under attack! Pray save me! (Robin Hood)

id1: Off (aborted)

id2: Fear not, friend Robin! I shall rout the Sheriff of Nottingham's men!

id3: Thank you, my good fellow! (Robin)

Each ghost-job would detect the fact that the other had been killed, and would start a new copy of the recently-slain program within a few milliseconds. The only way to kill both ghosts was to kill them simultaneously (very difficult) or to deliberately crash the system.

Finally, the system programmers did the latter... only to find that the bandits appeared once again when the system rebooted! It turned out that these two programs had patched the boot-time image (the /vmunix file, in Unix terms) and had added themselves to the list of programs that were to be started at boot time...

The Robin Hood and Friar Tuck ghosts were finally eradicated when the system staff rebooted the system from a clean boot-tape and reinstalled the monitor. Not long thereafter, Xerox released a patch for this problem.

I believe that Xerox filed a complaint with Motorola's management about the merry-prankster actions of the two employees in question. To the best of my knowledge, no serious disciplinary action was taken against either of these guys.

Several years later, both of the perpetrators were hired by Honeywell, which had purchased the rights to CP-V after Xerox pulled out of the mainframe business. Both of them made serious and substantial contributions to the Honeywell CP-6 operating system development effort. Robin Hood (Dan Holle) did much of the development of the PL-6 system-programming language compiler; Friar Tuck (John Gabler) was one of the chief communications-software gurus for several years. They're both alive and well, and living in LA (Dan) and Orange County (John). Both are among the more brilliant people I've had the pleasure of working with.

Disclaimers: it has been quite a while since I heard the details of how this all went down, so some of the details above are almost certainly wrong. I shared an apartment with John Gabler for several years, and he was my Best Man when I married back in '86... so I'm somewhat predisposed to believe his version of the events that occurred.

#### **Dave Platt**

Coherent Thought Inc. 3350 West Bayshore #205 Palo Alto CA 94303

--

Edited by Brad Templeton. MAIL, yes MAIL your jokes to funny@looking.UUCP Attribute the joke's source if at all possible. I will reply, mailers willing. Remember: If you POST your joke instead of mailing it, I will not reply.

## Stallman, Minsky and Drescher on the Internet Worm

<minow%thundr.DEC@decwrl.dec.com>
20 Dec 88 14:53

The following letter appeared in the Business section of the Boston Globe,

20 Dec 1988. [It does not represent the position of Digital Equipment Corporation (or my position, either). Martin Minow]

Recent computer virus threatens American justice system, too

The recent computer network virus was a prank designed to be harmless. A minor programming error made it replicate so much that it clogged Internet, a research network, with messages. Now some people want to punish this accident as deliberate sabotage.

Yes, people should not clog networks. But the "worm" had parts designed to avoid clogging; one had an error. Research is error prone: punishing errors is futile if limited to errors in pranks. More rational is to keep critical computers off research networks, as the military does.

Yes, another worm might be designed to destroy files. Some people are angry at these potential future crimes; so angry that they clamor to punish someone as an example, whether his own deeds deserve it or not.

This clamor threatens the American tradition of justice for each individual -- something even more valuable than a working Internet.

Richard Stallman Free Software Foundation, Cambridge.

Henry Minsky and Gary Drescher MIT Artificial Intelligence Laboratory, Cambridge.

# FAA Orders Computer Card Security Systems at 270 Airports

Henry Mensch <henry@GARP.MIT.EDU> Wed, 4 Jan 89 23:05:01 EST

(NY Times, 4 Jan 89) NEW YORK -- In a sweeping new move to tighten security at United States airports, the government Wednesday ordered that computer card systems be installed at the busiest terminals by early 1991 to keep people who might threaten airline safety from reaching restricted areas. Ultimately, a total of 270 airports would have to install either computer card systems, resembling those used for automatic banking, or alternative methods providing equal security. The Federal Aviation Administration rule, estimated to cost \$170 million over the next 10 years, was proposed in March.

The move was made as a result of the crash of a Pacific Southwest Airlines commuter jet in December 1987 that occurred after a passenger, believed to have been an employee dismissed by an that had bought PSA, fired several gunshots during the flight. All 43 people aboard were killed.

The decree Wednesday had additional significance in the aftermath of the bombing of a Pan Am jumbo jet over Scotland last month in which a total of

270 people were killed.

In a section of the rule justifying its action, the FAA said currently used identification badges "provide a means of control once an individual has gained access to a restricted area." "The FAA is concerned," it said, "that these procedures could allow an individual using forged, stolen or noncurrent identification to compromise the secured areas." It added that former employees could use their familiarity with procedures to enter a "secured area and possibly commit a criminal act on board an aircraft."

Burnley noted in Wednesday's announcement that computer-controlled card systems could be programmed to "keep a record of employees who try to enter areas for which they are not authorized." "They can also reject cards that have been reported lost or stolen, or which have not been surrendered by former employees," he said.

T. Allan McArtor, administrator of the FAA, said such systems already were in use at some airports and "have proved to be highly effective and workable."

Airline officials and airport operators had advanced many objections to the new rule, including the high cost of installing and operating the computer-card or other systems. But in dealing with the cost issue, the FAA said the total investment "can be recovered fully if one incident, involving the loss of 170 lives and a wide-bodied jet," were prevented in the next 10 years. [...]



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 8: Issue 3

# Sunday 8 January 1989

# **Contents**

Computer-related accidental death

Re: Danish Home Companion, Kierkegaard, and Feynman David E. Leasure

"NO CARRIER"

Jef Poskanzer via David Sherman

Re: Tales from the Vincennes tape

Mai. Doug Hardie

"Hand-written" letters

**Gary Chapman** 

Dark Side Hacker, an Electronic Terrorist

**Rodney Hoffman** 

The risks of trusting CBS

**Phil Goetz** 

Hackers - pure and simple

**Travis Marlatte** 

Viruses of all kinds

Travis Marlatte

Henry Cox's "Supercomputer used to `solve' math problem"

John C. Bazigos

Info on RISKS (comp.risks)

# Computer-related accidental death

<USER=GEGG@ub.cc.umich.edu> Sun, 8 Jan 89 15:27:28 EST

COMPUTER-RELATED ACCIDENT RESULTS IN WOMAN'S DEATH

JOHANNESBURG, SOUTH AFRICA, 1988 DEC 28 (NB) -- According to the Associated Press, a South African woman was killed Tuesday in a freak computer-room accident. The death occurred when 1 1/2-ton steel doors closed on Renata Espach as she stood in their path but out of sight of optical sensors intended to detect obstructions. The accident took place at the computer facilities of

Liberty Life in Johannesburg as the 23-year-old woman was handing a document to a colleague in the course of her employment.

found on usa today distribution bbs fido104/555 303-973-4222 1/7/89 by anonymous guest (no replies pls)

#### Re: Danish Home Companion, Kierkegaard, and Feynman (RISKS-8.1)

<hou2d!del@att.att.com>
Fri, 6 Jan 89 14:05:51 EST

R. P. Feynman in his recent book "What do you care what other people think" adapted a Buddist (possibly Shinto, I can't remember) story to explain dangers and benefits of technology. His explanation went something like this: There is a key that opens the gate of heaven and it's the same key that opens the gate of hell. The two gates cannot be distinguished from the outside and the only way to tell which is which is to open it. Obviously, it's very desirable to have this key because it allows us to experience wonderful things, but there's also the risk of hell. That key is technology.

David E. Leasure - AT&T Bell Laboratories - (201) 615-4169

#### ✓ "NO CARRIER"

David Sherman <dave@lsuc.UUCP> 6 Jan 89 07:57:49 EST (Fri)

| From: jef@ace.ee.lbl.gov (Jef Poskanzer)

```
| Newsgroups: comp.misc,comp.dcom.modems
| Subject: NO CARRIER
| Message-ID: <1595@helios.ee.lbl.gov>
| Date: 4 Jan 89 18:38:50 GMT
|
| Some terminal emulator programs have an amusing bug. When they see the | text "NO CARRIER" at the beginning of a line, they stop listening to | the modem. Like this:
| NO CARRIER
| If your emulator has this bug, you are no longer on line, and are not
```

If your emulator has this bug, you are no longer on line, and are not reading this. Yes, this sounds far-fetched, but I can personally assure you all that it's not just another chain-letter variation like the modem virus story. I discovered this on the WELL a while back when I opened a topic called "NO CARRIER", and then got mail from a user complaining that whenever he tried to read the topic his modem hung up. He was not computer-literate enough to have been making a joke. Recently another user reported the same problem.

Forwarded from Usenet by David Sherman, Isuc!dave@ai.toronto.edu

#### Re: Tales from the Vincennes tape

"Maj. Doug Hardie" <Hardie@DOCKMASTER.ARPA> Thu, 5 Jan 89 14:43 EST

I am not surprized by these relevations. I have observed the same behavior from my son when he is playing a video game on the computer. Once people get into these games, it is as if it was real, as if their life was threatened by whatever scenario is there. Perhaps games of that sort based on the particular equipment and expected mission could be used both in the development of systems to find out what strange things people will do under pressure, and to help train the eventual users to understand how to respond when those pressures do occur.

Doug

#### "Hand-written" letters

Gary Chapman <chapman@csli.Stanford.EDU> Thu, 5 Jan 89 09:14:37 PST

Jerry Leichter reported this item in an editorial of the New York Times:

The tide of progress, in other words, sometimes flows backward. There's probably only one sure way now to write letters that are, and look, personal: by hand.

Some years ago I was on the PBS television show \*Computer Chronicles\*, as part of a panel discussion about the use of computers in U.S. politics. The other guest on the show was a gentleman from a large direct mail firm which specializes in mailings for political causes and candidates. He brought along some of his samples to show us how sophisticated mailings are becoming. One of them was particularly interesting: the mailing was sent out to about three quarters of a million senior citizens in the state of Arizona. It had to do with some kind of issue that had an impact on senior citizens, and the polls indicated the vote was likely to be close (direct mail can make the difference only when votes are close). The direct mail company had developed a mail-merge program using handwriting instead of formed characters, and then had these letters printed on vast machines that actually wrote out the letters with high-speed pens, I gathered, so that the final product was virtually indistinguishable from a handwritten letter. The stationery the letters were printed on had only a person's name and home address at the top of the page, as if it were personal stationery. The envelopes were printed with the same handwriting sample and the same process so they appeared to be hand-addressed. The company even went so far as to affix the stamps (first class of course) on the outside of the envelope with a jig that rocked back and forth in a frame so the stamp would only rarely be glued on exactly straight up and down.

This gentleman from the direct mail company told us proudly that the campaign headquarters had received something like 14,000 telephone calls the first day after this mail was delivered, and the election was turned in their client's favor.

I looked at his sample letters and envelopes and could eventually tell that these were computer-generated. But I would not expect senior citizens, who typically don't imagine that technology is capable of simulating a hand-written letter so well, to be so discriminating. I would bet that a large majority of the recipients were convinced they had received a letter that someone had painstakingly written to them in a very personal fashion.

-- Gary Chapman, Executive Director, Computer Professionals for Social Responsibility

#### Dark Side Hacker, an Electronic Terrorist

Rodney Hoffman <Hoffman.ElSegundo@Xerox.com> 8 Jan 89 15:09:41 PST (Sunday)

Kevin Mitnick, earlier characterized as "armed with a keyboard and considered dangerous" [see <u>RISKS 7.95</u>] is the subject of a lengthy profile by John Johnson in the 8 Jan 89 'Los Angeles Times', with the headline:

Computer an 'Umbilical Cord to His Soul'
'DARK SIDE' HACKER SEEN AS 'ELECTRONIC TERRORIST'

When a friend turned him in and Mitnick asked why, the friend replied, "Because you're a menace to society." Mitnick is described as

25, an overweight, bespectacled ... computer junkie known as a 'dark side' hacker for his willingness to use the computer as a weapon.... whose high school computer hobby turned into a lasting obsession .... He allegedly used computers at schools and businesses to break into Defense Dept. computer systems, sabotage business computers and electronically harass anyone -- including a probation officer and FBI agents -- who got in his way. He also learned how to disrupt telephone company operations and disconnected the phones of Hollywood celebrities such as Kristy McNichol, authorities said.

So determined was Mitnick, according to friends, that when he suspected his home phone was being monitored, he carried his hand-held keyboard to a pay phone in front of a 7-Eleven store, where he hooked it up and continued to break into computers around the country. "He's an electronic terrorist, said [the friend who turned him in], "He can ruin someone's life just using his fingers."

Over the last month, three federal court judges have refused at separate hearings to set bail for Mitnick, contending there would be no way to protect society from him if he were freed.... Mitnick's lack ofconscience, authorities say, makes him even more dangerous than hackers such as Robert Morris Jr., ... who is suspected of infecting computer systems around the country with a "virus" that interfered with their operations.

Mitnick's family and attorney accuse federal prosecutors of blowing the case out of proportion, either out of fear or misunderstanding of the

technology.

The story details his "phone phreak" background, and his use of high school computers to gain access to school district files on remote computers, where he didn't alter grades, but "caused enough trouble" for administrators and teachers to watch him closely. He used the name `Condor,' after a Robert Redford movie character who outwits the government. The final digits of his unlisted home phone were 007, reportedly billed to the name "James Bond."

[He and a friend] broke into a North American Air Defense Command computer in Colorado Springs in 1979.... [The friend] said they did not interfere with any defense operation. "We just got in, looked around, and got out."....

What made Mitnick "the best" said a fellow hacker and friend, was his ability to talk people into giving him privileged information....

He would call an official with a company he wanted to penetrate and say he was in the maintenance department and needed a computer password. He was so convincing, they gave him the necessary names or numbers....

He believed he was too clever to be caught. He had penetrated the DEC network in Mass. so effectively that he could read the personal electronic mail of security people working on the case of the mysterious hacker and discover just how close they were getting to him. But caught he was, again and again....

Mitnick's motive for a decade of hacking? Not money, apparently.... Friends said he did it all simply for the challenge.... [His one-time probation officer says,] "He has a very vindictive streak. A whole bunch of people were harassed. They call me all the time." .... His mastery of the computer was his "source of self-esteem," said a friend.

### The risks of trusting CBS

<PGOETZ@LOYVAX.BITNET> Sat, 7 Jan 89 15:03 EST

From the Jan. 89 issue of The Institute (a supplement to IEEE Spectrum), in an IEEE article by Tekla Perry:

Saratoga, CA- Some 200 personal computer industry pioneers and current innovators met here Oct. 7-9 for the invitation-only fourth annual Hackers Conference...

"Hackers," as defined by this group, are "artists of technology," people who "derive joy from discovering ways to circumvent limitations," or more simply, those who are willing to "hack at that computer keyboard until the computer does what you want it to."

[Note that people invited to the Hackers Conference include people like Steve Wozniak, Bill Gates, Mitch Kapor, etc. (as well as CBS!). Imagine their surprise when , according to the article:] CBS... seemed not to have taken the point. Its Oct. 8 national report led with these words: "A small revolutionary army is meeting in the hills above California's Silicon Valley this weekend, plotting their next attack on the valley below..."

Phil Goetz PGOETZ@LOYVAX.bitnet

### ✓ Hackers - pure and simple

<att!ihlpa!travis@ucbvax.Berkeley.EDU> Fri, 6 Jan 89 14:05:08 PST

I hold a more elementary definition of "hacker". One that was applicable in the early days and remains so. Very simply, a hacker is one who is keenly interested in the full capabilities of a system. This implies that experimenting is done to discover the undocumented features, the limits of the controls, and the back doors that should not exist. This was and can be done in a constructive way. This was and can be done in a malicious, irresponsible way.

We, as computer professionals have, then, two responsibilities. First, we must begin to think of malicious hacking as socially unacceptable. This should not require the demise of hacking (according to my definition) altogether. The perpetrator of misdirected hacking must not be rewarded for his or her efforts. As colleagues of the irresponsible hackers, we must view them with distaste for they will destroy the profession.

Second, a system of licensing should be implemented. This need not be (but could be) a knowledge certification. A general form of permission granted to all who request it would suffice. This license can then be revoked or suspended upon conviction of some computer related offense. The license number would be put on resumes, employers would demand new employees to have valid licenses, and the future of ones career would hinge upon keeping that license intact.

The public has a right and, unfortunately, a need to regulate computer related activity that affects the public. Some sort of licensing proclaims that society agrees that this person is trustworthy (so far). Mr. Morris, Jr. would not, in my eyes, be eligible to receive a license to practice his trade.

Travis Marlatte ihlpa!travis 312-416-4479 AT&T Bell Labs

#### Viruses of all kinds

<att!ihlpa!travis@ucbvax.Berkeley.EDU> Fri, 6 Jan 89 14:44:20 PST

The analogy between computer viruses and medical viruses is appropriate. Medical researchers are required to use approved methods for biological research. The leverage enacting those requirements comes in the form of: licensing by a medical board with a list of expectations, laws that protect the public's safety, and even laws that protect animal rights.

There is nothing to stop a researcher from suddenly going mad and applying his or her knowledge for malicious purposes. There is incentive to follow socially approved channels for conducting legitimate research - fear of losing one's license or being criminally charged. With these mechanisms and laws in place, the public has a means to deal with malicious researchers who ignore the rights of others.

Travis Marlatte ihlpa!travis 312-416-4479 AT&T Bell Labs

## ★ Henry Cox's "Supercomputer used to `solve' math problem"

"John C. Bazigos" <bazigos@cd7.ics.uci.edu> Thu, 05 Jan 89 19:59:44 -0800

> Date: Wed, 21 Dec 88 09:23:26 est

> From: Henry Cox <cox@spock.ee.mcgill.ca>

> Subject: Supercomputer used to "solve" math problem (RISKS-7.97)

The "Montreal Gazette" errs by espousing the false belief that solving "a theoretical mathematics problem so complex that it is beyond the capability of the human mind to comprehend" implies, first, that scientists must "accept the supercomputer's solution more or less on faith"; and second, that the proof is not fully understandable for verification purposes. The necessary and sufficient condition for verifying a proof is ensuring that each step in the derivation of the final result is valid -- i.e., follows from formal definitions, postulates, rules, and validly derived results (i.e., lemmas and/or theorems). However, that condition is neither necessary nor sufficient for understanding the problem: One can, trivially, logically derive a result that one does not "comprehend"; and inversely, one can comprehend a result, whether it is true or false, for which no derivation is known --e.g., P being a strict subset of NP, or Fermat's "Last Theorem"-- or for which no derivation exists -- e.g., Godel's reflexive assertion of not being a theorem. The only faith required to verify any proof is faith in, first, the logical system on which the verification is based; and second, the verification's valid stepwise application of that logical system. Summarily, one not only can, but logically must, accept the result of validly applying valid logic to premises that one accepts, regardless of the extent to which (s)he "comprehends" the result.

Now, if my information that the (non-)existence of a finite projective plane of order 10 does not qualify as "a theoretical mathematics problem so complex that it is beyond the capability of the human mind to comprehend" is correct --which seems likely, given that humans programmed the computer to (dis)prove it-- then the article was blatantly inaccurate in characterizing the problem as incomprehensible. However, whether or not the argument was thus falsely predicated, its logic was, as proven in the immediately preceding paragraph above, invalid -- and non-trivially so, as Mr. Cox's above inferences therefrom demonstrate.

In response to Mr. Cox's terminal (parenthetic) sentence

> [ The RISKS are obvious. The willingness of people to accept a computer's

> answer on faith (whether at the cash register at the grocery store or in the > university environment) remains disturbing. Henry Cox]

it would be disturbingly anti-progressive of people to continue to trust human operators more than non-human machines to perform tasks (e.g., tabulating grocery bills, and operating switching networks) that these machines have proven themselves superior to humans at executing.

Verifiably yours, -- John C. Bazigos

P.S. Given that the earth's present population is less than 5 billion; it follows that 1 quadrillion possibilities represents 200,000 possibilities per person -- which is 4 times the above article's claim of 50,000 per person.



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 8: Issue 4

## Wednesday 11 January 1989

## Contents

M1 Plane crash

**Nigel Roberts** 

\$4.5 M Child Support Computer to be Scrapped in VA **Dave Davis** 

Eelskin wallets erase mag strips?

Jane D. Smith

Firearms Arrive in the Electronics Age

Unused city computer system set aside after 4 years, \$4M Stephen W. Thompson

Re: Hackers' Conference versus CBS John Gilmore

Info on RISKS (comp.risks)

#### M1 Plane crash

Nigel <roberts%untadh.DEC@decwrl.dec.com> Wed, 11 Jan 89 03:02:40 PST

"DISASTER BECOMES A MATTER OF ROUTINE

There is no pattern to the proliferation of disasters. Lockerbie was a bomb on a middle-aged jet, blown to pieces high over a Scottish town. Flight BD-92 was a spanking new jet which somehow (inevitable speculation) seems to have contrived to lose both engines limping in to land at Castle Donington. No suggestion of a bomb, though the flight was Belfastbound; and --- compared to the carnage of Lockerbie --- enormous strokes of good fortune. You cannot, surveying the debris strewn across the M1 (freeway), quite visualise how so many passengers survived, nor calcualte the odds against the doomed Boeing ploughing into a string of cars and lorries; nor those against fire engulfing the scene.

In a way, the horror of BD-92, like Clapham Junction, like King's Cross even, is easier to come to terms with. It was justone of those things:

mechanical (or, possibly, human error.) Inquiries may be conducted, reports published. There are things that can be done. Engines to be checked. Software to be scrutinised. Training to be tightened. And, beyond such simple reactions, of course, there will be more political questions. How rigorous and independent are Civil Aviation Authority checks? Do they take too much for granted, because the FAA has already pronounced an aircraft safe? Have all the lessons of Manchester been learned and acted upon? What are the risks for two engined planes? We have been constantly informaed that the chances of both engines failing are millions to one, so that such airliners now cross the Atlantic as a matter of routine. But the odds may have shortened somewhat over Kegworth on Sunday night.

There is a broader sense, though, in which the M1 disaster brings no comfort at all. It was a failure of technology; or maybe some element of human incapacity to deal with technology. There is supposed reassurance in hi-tech. The machines take over, to blind-land a jumbo, or put man into space. Eliminate human error. Leave it to the computers. But that is too blithe. Week after week, month after month, hi-tech planes fall out of the sky. Because they are military jets, and fall usually into the sea or on some deserted hillside, they do not command the headlines. (Though when, as a few weeks ago, they plough into the centre of a West German town, all that changes). They are not safer because of their extreme sophistication; on the contrary, they are dangerous because human beings, no matter how relentlessly trained, are not sophisticated enough to command their infinite complexity. And so, in civil aviation too, the new, replacing the middle aged, does not automatically spell greater safety.

We must, in short, begin to budget for disaster. Watch the jets stacked over Heathrow or Gatwick and there is a feeling of living dangerously, of disasters waiting to happen. As they occur, they will not necessarily alter the basic calculations. It will still, statistically, be safer to take a flight to New York, than your car for a Sunday spin. The growth in air traffic cannot be checked; nor can the demand for new, more complex planes. There is, here, a sense of challenge. Airports within a few hundred yards of motorways; jets wheeling to land over cities. Lockerbie and Castle Donington are very different cases, united only by their fear and pity. The odds against them happening with a handful of days, like the odds against two engines failing, were millions to one. But disaster, it seems, has a way of rendering odds meaningless."

--- 'The View from Britain', leader article in \_The Guardian\_ newspaper, Tuesday January 10 1989

[Several of this evening's news programs report the possibility of a computer problem or cross-wiring error that might imply it was not pilot error... PGN]

#### ★ \$4.5 M Child Support Computer to be Scrapped in VA

dave davis <davis@community-chest.mitre.org> Wed, 11 Jan 89 07:54:07 -0500 From the 24 Dec 88 issue of the Washington Post comes an article about yet another failed software development project.

The system was to disburse child support payments for the State Dept. of Social Services...The state paid \$4.5 M for the system in 1985... problems with the system caused delays up to six months in issuing payments...

The state is now seeking a completely new system [now that it has figured out its requirements, apparently] for \$10M, to be installed in two years.

The article further states: "the state bought Unisys' proposed package outside of normal competive bidding practices, a move a state auditors' report later found was made in an 'atmosphere of panic and haste'...welfare officials never checked to see if the system would do what the company promised."

It appears that the state officials involved didn't exercize the kind of management care that a more routine non-technical procurement would have received.

Dave Davis, McLean, VA

#### ✓ eelskin wallets erase mag strips?

Jane D. Smith <jds@uncecs.edu>
10 Jan 89 15:44:03 GMT

From a report on NPR's All Things Considered program 1/9/89:

A spokesperson for a distributor of eelskin wallets responded to the apparently widespreading rumor [SEE RISKS-6.25] that eelskin wallets erase the magnetic strip information on credit cards and ATM cards of their owners. Sales of eelskin wallets have dropped as wary consumers boycott the alleged mag strip eaters. The magnets used as closures for the wallets are the real culprits, however, and the spokesperson said the manufacturers were now using smaller magnets as closures or using conventional snap closures. Caveat emptor!

-- Jane Dunlap Smith UNC-ECS Information Services

#### Firearms Arrive in the Electronics Age

<aLLEN@s56.prime.com> 10 Jan 89 11:30:27 EST

This item appeared in Business Week Nov 28, 1988:

Electronic Gun

Colt industries Inc has filed for US and European patents on a handgun with an electronic firing system. Pulling the trigger would move a magnet past the solid state switch, triggering a circuit that releases the hammer. It would be more reliable and cheaper than mechanical systems, says the company.

In addition, putting chips in pistols would make it possible to add a digital display that warns when the gun is loaded and shows how many shots are left. And that could just be the beginning of new "user friendly" features for tomorrow's firearms.

Now, I'm not a "hardware type" (maybe they're thinking of microcoding the gun :-)?), but after reading recent RISKS articles that discuss such things as electromagnetic interference with army helicopters, etc., it seems that the risks attendant with the device described above should be prohibitive. This firearm design seems just plain absurd!

Other points: whatever happened to the tried-and-true engineering philosophy of "simplest best"? An electronic firing system in a handgun seems, say, Rube Goldberg-ish, yes? Furthermore, with your little digital display, all the excitement of playing Russian Roulette would disappear.

-----

Date: Mon, 09 Jan 89 15:07:47 -0500

From: "Stephen W. Thompson" <thompson@a1.quaker.upenn.edu>
Subject: Unused city computer system set aside after 4 years, \$4 million
Organization: Institute for Research on Higher Education, Univ. of Pennsylvania

The following article comes from the 6 January 1989 (Friday) Philadelphia Inquirer, front page. In this city where the government is widely criticized on every front, it raises questions of incompetence and poor management. It also, however, raises questions about whether cities out to be involved in software development.

Unused city computer system set aside after 4 years, \$4 million By Dan Meyers, Inquirer Staff Writer

After at least \$4 million in expenses and more than four years of frustration, the City of Philadelphia has shelved a computer system it bought -- but never used. Officials in the Finance Department had pitched the system in the early 1980s as an efficient way to track information on payroll, pensions and personnel.

"Has it worked?" City Councilman John F. Street asked at a hearing this week.

"No it has not," said Deputy Finance Director Peter A. Certo, the latest supervisor of the project. Certo said the total cost has been at least \$4 million. Street put it at \$5 million. The system now is in storage.

For the current fiscal year, which began in July, the Finance Department had budgeted more than \$400,000 for a 13-member team to work on the computer system.

\* In May, however, with Mayor [Wilson] Goode facing a \$79 million budget deficit and calling for a cut of 2,000 people in the city workforce, Finance director Betsy C. Reveal decided to put the program on hold indefinitely. She did not respond to requests for comment.

"We didn't really scrap it," said Certo. "We put it on the back burner."

Records in the city controller's office show the project was scuttled by mid-September. The failure of the system was mentioned Wednesday in a hearing on another matter of the Appropriations Committee, which Street chairs.

"Council members really though we'd been burned" on the Finance Department project, Street said.

\* [Overall problems with city funding finally brought the computer system's development to a halt.]

The computer tapes, programs and consultant reports have been put in storage and could be "resurrected" when the city can afford to pursue them, Certo said. Certo said the problem was that it was difficult to adapt a computer system to the myriad peculiarities of the city. And he said it would have taken additional staff and money to get the computer system working. According to Certo, the project was underfunded from the start. When it was mothballed, the computer program was at least six months away from working, Certo said.

Others were skeptical of the ability of such departments as Finance to oversee complicated computer projects. "Systems like this are difficult to install and should be left to professionals to do," said Eugene L. Cliett Jr., director of the Philadelphia Computing Center, an office created by Goode to oversee city computer projects.

The computer project was under discussion at least as early as 1982, under the administration of Mayor William J. Green, according to controller records.

The plan was to take a software package -- computer programs already designed by a company -- and modify it to the city's particular needs. The city chose not to order a custom-designed computer system because the cost would have been double or triple, Certo said.

By early 1984, the city had entered into a \$1.4 million contract with American Management Systems to develop a computer system that would combine, in easily digestible form, data on city employees.

"Time is of the essence," the contract said.

Numerous consulting contracts followed, totalling at least \$214,000, according to controller records. Much of the rest of the cost was for city staff assigned to the project.

The system initially was to include information on three areas -- payroll, pensions and personnel. All had, and still have, separate computer systems. The pension board pulled out of the project shortly after it began.

"We have a system now that is 30 years old and it pays people every week but doesn't give us a lot of management information we'd like to have," Certo said. The computer system that was supposed to cure that problem was slow in taking shape, however. "We spent two years modifying the package and in the course of that period found things we felt wer not addressed adequately by AMS," Certo said. At one point, he said, the list of problems was at least 85 items long.

AMS consultants began to phase out of the work and the city Finance Department took it over. But one department or another objected to the results, Certo said. "We were constantly changing things," he recalled. "We tried to accommodate everyone."

Finally, in the city budget crunch, Reveal decided to abandon the long-standing project, at least for the moment.

So at a time when the city could most use precise information that could help the city run more efficiently, the Goode administration has determined that it cannot afford to pay for it.

"You're damned if you do and damned if you don't," Certo said. "We decided not to do it."

#### Re: Hackers' Conference versus CBS

John Gilmore <gnu@toad.com> Mon, 9 Jan 89 18:13:34 PST

I was at the Hackers' Conference whose blatantly slanted news coverage was recently reported in The Institute and Risks. I created a transcript of the CBS news segment the evening it was aired; it is below. Reading it is interesting; while CBS never lied, they juxtaposed material from different sources to make a strong impression that we were criminals. Note in particular what was happening on the screen while various things were said (e.g. showing a "combat" video game while talking about us as revolutionaries, showing Cliff Stoll giggling about mice and playing with a Yo-Yo). BTW, there \*was\* the obligatory shot of tape drives, I seem to recall.

CBS was given special access in order to film the conference; the rest of the press was only allowed there on Sunday. Needless to say they will NOT be invited back (and I will personally escort them off the property even if they show up on Sunday). Unfortunately, that's not enough. The producer of the show guaranteed that the attendees' image of hacking, rather than the distorted, media-generated image of hacking, would be presented. He broke that promise, with a vengence, but boycotting CBS won't help. (Fred Peabody produced the Hackers coverage. He went to ABC, working on 20/20, according to Glenn Tenney, who ran the Hackers Conference. Be sure you don't let him \*near\* anything you are doing -- if you want fair and unbiased coverage.)

John Gilmore

Transcript of CBS News segment on the Hackers Conference filmed 7 Oct 88, aired 8 Oct 88.

Anchorman ("High Technology" logo and drawing of chip): An unusual conference is under way near San Francisco. The people attending it are experts on a technology that intimidates most of us, but has changed the way we live. John Blackstone reports.

Narrator (trees and outdoor scenes at conference): A small revolutionary army is meeting in the hills above California's Silicon Valley this weekend, plotting their next attacks on the valley below, the heart of the nation's computer industry. They call themselves computer hackers.

Jonathan Post: "The people who are gathered here changed the world once; if we can agree on where to go next, we're gonna change it again."

Narr (conference scenes, blinking lights): What hackers have learned to do with computers has changed the world, for both good and bad. They're the people who dreamed of and built the personal computer industry. But the same kind of talent is creating never before dreamed-of crime. Because for a computer, the only difference between a hundred and a million is a few zeros.

Donn Parker, (SRI International, in office): "And so, in fact, criminals today I think have a new problem to deal with: and that is how much should I take. They can take any amount they want."

Narr (phone central office): Telephone companies are the most victimized because those who break into phone company computers can link up for free to computers around the world.

Richard Fitzmaurice (Pacific Bell, in office): "You'll hear the term computer hacker, computer cracker; we call them computer criminals."

Narr (blinking lights): But much more frightening are the hackers who crack American military computers. Earlier this year in a lab that does some classified research, astronomer Clifford Stoll discovered someone had broken into his computer. He says it was like finding a mouse running across the floor.

Stoll (in office): "You watch and you see, he's going in that hole over there, and you say, ooh, he's going in that hole; that connects to a network that goes to a military computer, in Okinawa."

Narr (Stoll playing with a yo-yo in a machine room): The breakins to American military computers went on for several months. Eventually Stoll traced them to a hacker in West Germany.

Donn (in office): "A hacker today is an extremely potentially dangerous person. He can do almost anything he wants to do in your computer."

Narr (at conference, video games, stabbing and fighting on screen): But at the hackers' camp in the hills, there's recognition that in any revolutionary army there will be a few rogues and criminals. But that's no reason, they say, to slow down the revolution.

"John Blackstone, CBS News, in the hills above Silicon Valley."



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 8: Issue 5

## Wednesday 11 January 1989

#### Contents

- Digital Photos and the Authenticity of Information **Dave Robbins**
- Medical software **Ivars Peterson via Robert Morris**
- Info on RISKS (comp.risks)

## Digital Photos and the Authenticity of Information

Dave Robbins <dcr0%uranus@gte.com> Mon, 9 Jan 89 10:53:43 EST

An article in the Boston Globe on January 2, 1989 describes the use of digital technology to retouch or drastically alter photographs, with results that show no evidence of the fact that alterations were done. The article said: "The 80's are fast becoming the last decade in which photos can be considered evidence of anything." It pointed out that the only confidence we can have in these digital photographs relies upon the ethics of the people who use the machines. In response to the question: "What about the ethics of all this?" a vendor of the technology is quoted as answering: "That's up to you." George Wedding of the Sacramento Bee is quoted as saying: "I hope that 10 years from now readers will be able to pick up a newspaper and magazine and believe what they read and see. Whether we are embarking on a course which will make that impossible, I don't know. I'm afraid we have."

This is not the first time I've read about this technology, and every article I've read has raised the concern that the new technology renders inoperative a very basic assumption made by society (and the law, in particular) since the development of photographic technology; namely, that a photograph can be considered to be reliable evidence. Until recently, it was virtually impossible to alter a photograph without leaving evidence of the alteration; physical evidence was available to confirm or deny the authenticity of the photo. With digital photos, this is no longer true.

The article reminded me, however, of a more basic concern I have regarding

the use of computer technology. Computer technology has had the following impacts upon record-keeping:

- 1) The use of electronic storage to eliminate physical storage (e.g., paper) of information has certain clear benefits, but has also eliminated reliable records of that information, because electronic storage media can be altered without leaving any evidence of alteration. Electronic records cannot be considered to be as reliable as physical records (certainly not today, and perhaps not ever). The best we can do is provide a combination of physical security and software controls to attempt to assure the reliability of records; and as we all know, software controls are not all that reliable and in any case can be circumvented, often with the greatest of ease.
- 2) Computer technology renders the task of altering electronic records extremely easy. Forgery has been a problem ever since written records were first used. But before computer technology was used to store and manipulate records, few people were capable of forging records well enough to fool anyone else -- forgery of physical records requires a considerable skill, possessed by relatively few people. Successful alteration and forgery of electronic records, however, requires considerably less skill -- and the skill it does require is usually one that a large number of people possess: the ability to use a computer.
- 3) Computer technology has made it practical to store and manipulate far larger volumes of information than could be handled with prior technology. We have no practical means of verifying the integrity of such large volumes of information, and are thus left with no choice but to trust that the electronic records are accurate. It is wholly impractical, for example, for the Social Security Administration's entire data base (how many hundreds of millions of individual records?) to be manually audited to verify its accuracy.

What bothers me is the combination of factors: the electronic storage of the information makes it very easy to carry out successful alterations and forgeries, and the volume of information makes it practically impossible to verify the authenticity of the information. As we put more kinds of information under the control of computer technology, it seems to me that we make it ever more difficult to trust the authenticity of information. Computer technology has the potential (and is in fact beginning to realize that potential) to destroy the very important and fundamental concept that truth is ascertainable from physical evidence.

Are we approaching the point (or have we reached it already?) where truth is, for all practical purposes, whatever the computer says it is? Where what is accepted as truth is easily manipulated by those who are privileged to have access to the digital keepers of truth?

We observe a bit of this phenomenon in advertising (commercial and political), where public perception of truth is subtly manipulated by images and propaganda; and to that extent, this is not a phenomenon peculiar to computer technology. But most of us are at least aware that advertising is on the face of it an attempt to persuade us to believe a certain thing, and thus that its appearance of "truth" is not to be taken at face value. We at the

same time continue to believe that facts are facts, and that there are reliable ways to permanently record objective truth.

The computer is depriving us of the ability to authenticate that which is purportedly a recording of objective truth. What will the impact be upon society when we come to understand that we can no longer trust those forms of evidence that we have so long taken for granted to be reliable? When an authentic-looking photograph shows something that may or may not have actually existed? When an apparently authentic sound recording reproduces sounds that may or may not have actually occurred? When a corporation's audited and verified financial records describe financial activities that may or may not have ever occurred?

Not that these are really new threats: individuals have for a long time attempted to falsify all kinds of records. But in times past, it has been so difficult to succeed at forgery that we have been confident that a forgery could be detected. That confidence leads to the confidence that if a physical record passes all authenticity tests, it is indeed a reliable record.

Computer technology has destroyed this confidence. Where are the authenticity tests for electronic records? Is it ever possible for us to have the same high degree of confidence in electronic records that we have in physical records? I understand software too well to suppose that today's software technology is capable of supporting really trustworthy verification of the authenticity of electronic records, and I'm not convinced that software can ever be trustworthy enough to achieve the level of reliability possessed by physical records. But does that mean that we shouldn't use computer technology to manage information? How do we in the computer industry deal with this problem?

#### Medical software

<RMorris@DOCKMASTER.ARPA>
Tue, 10 Jan 89 12:04 EST

A Digital Matter of Life and Death by Ivars Peterson Science News, 12 March 1988

The radiation-therapy machine, a Therac 25 linear accelerator, was designed to send a penetrating X-ray or electron beam deep into a cancer patient's body to destroy embedded tumors without injuring skin tissue. But in three separate instances in 1985 and 1986, the machine failed. Instead of delivering a safe level of radiation, the Therac 25 administered a dose that was more than 100 times larger then the typical treatment dose. Two patients died and a third was severely burned.

The malfunction was caused by an error in the computer program controlling the machine. It was a subtle error that no one had picked up during the extensive testing the machine had undergone. The error surfaced only when a technician happened to use a specific, unusual combination of keystrokes to instruct the machine.

The Therac incidents and other cases of medical device failures caused by

computer errors have focused attention on the increasingly important role played by computers in medical applications. Computers or machines with built-in microprocessors perform functions that range from keeping track of patients to diagnosing ailments and providing treatments.

"The impact of computers on medical care and the medical community is the most significant factor that we have to face," says Frank E. Samuel Jr., president of the Health Industry Manufacturers Association (HIMA), based in Washington, D.C. "Health care will change more dramatically in the next 10 years because of software-driven products than for any other single cause." Samuel made his remarks as a recent HIMA-sponsored conference on the regulation of medical software.

At the same time, reports of medical devices with computer-related problems are appearing more and more frequently. In 1985, the Food and Drug Administration (FDA) reported that recalls of medical devices because of computer faults had roughly doubled over the previous five years. Since then, the number of such complaints has risen further.

The problems range across a wide spectrum of computer-based medical devices. A system designed for monitoring several patients at once was recalled because it kept mixing up the patients. A programmable heart pacemaker suddenly "froze" while it was being adjusted by a doctor. A device for dispensing insulin delivered the drug at an inappropriate rate. An expert system gave the wrong diagnosis, resulting in a patient receiving a drug overdose. An ultrasound scanner sometimes underestimated fetal weight.

"No one can deny that allowing computers to perform some of the functions normally carried out by trained and licensed medical professionals raises questions concerning the personal health and safety of citizens," Michael Gemignani of the University of Maine in Orono comments in ABACUS (Vol. 5, No. 1). "But even if we agree something more needs to be done to protect society in the face of these technological innovations, we are still left with the question: What should be done and by whom?"

The FDA, in its mandated role as guardian of public health and safety, is now preparing to regulate the software component of medical devices. The agency's effort has already raised questions about what kinds of products, software and information systems should be regulated.

Last fall, the FDA published a draft policy for the regulation of computer products marked for medical use. In that policy, the concept of "competent human intervention" sets the dividing line between what is and is not regulated. In other words, the computer product in question is subject to regulation if a qualified doctor or nurse cannot effectively intervene to override the machine's actions. Devices such as software-driven cancer therapy machines, programmable heart pacemakers and automatic drug dispensers clearly fall into that category.

On the other hand, the FDA states that it would not regulate computer products that simply store, retrieve and disseminate information analogous to that traditionally provided by textbooks and journals. In addition, the agency's regulations would not apply to computer products used only for communications, general accounting or teaching.

For example, a physician may use a computer program known as an expert system to help make a diagnosis. Because the expert system does not directly drive another medical device that, say, could dispense a drug when needed, and because the doctor can make an independent judgment, such an expert system would be exempt from FDA rules governing medical devices.

However, the greatest advantage of software - its flexibility - is also, from a regulatory point of view, one of its biggest problems. Computer

programs are easy to change and can be used in many different ways. If corrections are made or new features added, how much scrutiny should the modified version of a previously approved computer product undergo? That question is still unresolved.

Furthermore, it's sometimes hard to make a clear distinction between programs that perform a "library" function and those that can be classified as being part of a medical device. A case in point is the patient medical record, traditionally a file folder containing various sheets of paper listing treatments, medical observations and other pieces of information vital for the patient's proper care.

Many hospitals are now moving toward medical records that are stored on a computer. The difficulty arises when such information systems are connected directly to machines that, for example, record patient blood pressure and heart rate. If a nurse takes down the data and then enters the figures into a computer, the information system software would not be subject to FDA rules. But if the machine sends the data directly to the computer, then the information system is considered by the FDA to be an "accessory" to a medical device and subject the same level of regulation as the machine itself.

Information system vendors disagree with the FDA's position. They argue that the FDA does not presently have rules governing the quality and content of paper medical records. There's no reason for the FDA to start regulating such records, they say, just because the records happen to be in a computer's memory rather than on paper. In fact, using a computer-based system would dramatically reduce the incidence of errors in patient records, the vendors claim. The benefits of improved record keeping would clearly outweigh the need for burdensome regulation.

The FDA's James S. Benson concedes that "regulation is not the automatic solution to problems in hospitals and elsewhere." Nevertheless, the agency must comply with a 1976 law that contains a broad definition of what constitutes a medical device. Interpreted in its broadest sense, the definition encompasses practically everything used in a hospital, from X-ray machines to pencils.

FDA officials say they recognize the difficulties involved in regulating medical software. "The agency fully appreciates the revolution occurring in medicine with the introduction of computers and microprocessors," says Frank E. Young, FDA commissioner. "We're taking a reasoned, structured approach with a minimum of oversight. We have tried to give general guidelines. The policy has been deliberately made flexible."

The flexibility allows the FDA to consider applications for approval on a case-by-case basis. That limits the "chilling fear of undue regulation," says Young. Furthermore, as technologies change and experience with computers in medical applications grows, decisions on how much regulation is needed may also change.

To many manufacturers and users of medical products, the FDA's idea of flexibility leaves too much uncertainty and opens up the possibility of increased regulation in the future. "The FDA casts too wide a net," says Edward M. Basile of King & Spalding, a law firm in Washington, D.C. "Their basic assumption is that everything should be regulated."

"There's no disagreement about the extremes," says Harold M. Schoolman of the National Library of Medicine in Bethesda, Md. "The question is how and where to draw the line between the extremes." The important issue, he says, is maintaining a balance between appropriate safeguards and incentives for innovation.

Even in situations where it's clear that certain software ought to be reviewed, the FDA faces the additional difficulty of how to go about verifying that a particular computer program does what it's supposed to do -- nothing more, nothing less. As experience with software for other applications has shown, the task of checking software quality can be overwhelming (SN: 9/13/86, p. 171).

A few years ago, when most medical devices did not contain computers, it was relatively easy to foresee all possible inputs and to check the consequences of each one, says James Howard of General Electric's Medical Systems Group in Milwaukee, Wis. With computers, the number of possible paths is greatly increased. "It's more important than ever to build safe products that perform as required," he says. But because a detailed analysis takes so long, it often can't be done. "This is a major concern to both manufacturers and the FDA," says Howard.

The FDA defines software as a "set of instructions that enables a computing machine to control, monitor or otherwise interact with a medical device." The proposed regulations require a software developer to show that the algorithm, or mathematical recipe, used in the computer program is appropriate and has been implemented correctly in the software. The FDA also requires assurance that any software failure would not injure the patient.

How that assurance can be provided is still unclear. Techniques for evaluating software safety are relatively new. Who does the checking, how much evidence is enough and whether the FDA can perform an independent check are also unresolved issues. Furthermore, software developers are wary of submitting complete listings of the instructions in their computer programs because competitors may get a look at this "source code" by making a request to the FDA under the Freedom of Information Act.

The trouble with the FDA approach, says Howard, is that it doesn't consider under what conditions software is used. Instead, the FDA ought to focus on the idea that not all computer errors are equally serious. Using a kind of hazard analysis to focus on situations that could lead to life-threating computer failures would be one way to eliminate the most serious potential faults and to shorten testing times.

Software developers also need to improve the methods they use for constructing computer programs. We need to "industrialize" software development so that programs are written in a consistent way, says James Dobbins of Verilog USA, Inc., in Alexandria, Va. Too often, programmers include a description of what each part of a program does only as an afterthought. They rarely go back to clean up or polish a program to make it more understandable.

Software development can be standardized and automated, says Dobbins. "The tools are there to industrialize the whole process. You just have to go find them."

Programmers, on the other hand, complain that they're in a no-win situation. Software is continually modified as it evolves, often to meet demands for new features to make the product more competitive. In the rush to market, when delays can put a company at a competitive disadvantage, software testing often loses out. Delays in completing a software package are balanced against the possibility of failing to root out potentially embarrassing errors.

This is the kind of situation that can lead to lawsuits, says Vincent Brannigan, an attorney in Adelphi, Md. Software is clearly a product, he says. If it's defective and injures a consumer, then the manufacturer is liable.

Among the faults Brannigan lists is the tendency of software and computer companies to promise more than they can fulfill and to cut costs by doing less

testing. This is the only field, he says, where the customer is expected to pay for finishing a product through the purchase of periodic updates and corrections to the software.

"Disclaimers don't mean anything," Brannigan says. "The product should have been right in the first place." That means paying much more attention to how software is written and tested. "The software must look as shiny and clean as the rest of the machine," he says.

So far, software developers have generally escaped damaging lawsuits and settlements, but that may change. To many medical-device producers, the threat of litigation may be even more effective than proposed FDA regulations for assuring the quality of products.

Even finding out what went wrong is a time-consuming process. The FDA and other groups are still investigating aspects of why the Therac 25, manufactured by Atomic Energy of Canada Ltd. in Kanata, Ontario, failed. What's evident is that the problem could probably have been avoided if an appropriate safety analysis had been done.

The Therac 25 delivers two forms of radiation: either a high-energy electron beam or, when a metal target intercepts the electron beam, a lower-energy X-ray beam. It turns out that when a nimble, experienced technician punches in a particular sequence of commands faster than the programmers had anticipated, the metal target fails to swing into place.

A safety analysis would have identified the missing target as a potentially dangerous situation. The machine could have been programmed so that it couldn't operate if the target, as confirmed by a sensor, were not in place.

Perhaps such a complex, computer-driven machine wasn't even necessary. By sacrificing a little convenience and flexibility, a machine with a simple on-off switch and a timer could probably have done the same job - with a much smaller chance of failure.

[This is a familiar topic to RISKS readers, but this particular article is extremely well written and seems worth including, even if old. (RISKS has reported one additional death involving the Therac.) 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 8: Issue 6

## **Thursday 12 January 1989**

#### Contents

Computers and Civil Liberties, article by Gary Marx

Ronni Rosenberg

Losing systems

**Vince Manis** 

Our blinders [with respect to RISKS]

**Don Alvarez** 

Totally secure MAIL & infallible aeroplane warning systems **Nigel Roberts** 

"Disaster Becomes a Matter of Routine"

Steve Philipson

Re: Biased coverage of hacker's convention by CBS Richard Thomsen

SAFECOMP89

**Udo Voges** 

Name this book -- for a box of cookies! **Cliff Stoll** 

Info on RISKS (comp.risks)

#### Computers and Civil Liberties, article by Gary Marx

Ronni Rosenberg <ronni@juicy-juice.lcs.mit.edu> Thu, 12 Jan 89 13:07:11 EST

"This is the year of spying kits for kids," by Gary Marx

In a popular song Paul Simon tells us that 'these are the days of miracle and wonder.' Surely this is so for the lucky child faced with a cornucopia of computer and other electronic toys this holiday season. But among the games and educational tools is one category that should give us pause: spy toys.

In one catalogue, under the heading 'Toys to Grow On,' for \$19.95 you can have Super Ears, which 'help you detect even the slightest sounds! Slip on the headset and aim the disk; even if your target is far away, you'll hear every rustle, every footstep, every breath, and every word!' Another

stethoscope-like device permits you to hear 'quiet breathing, through a concrete wall a foot thick' and with 'fidelity good enough to record.' And for only a few dollars, stockings can be stuffed with a Dyna-Mike Transmitter; smaller than a quarter, it 'will transmit every sound in a room to an FM radio tuned to the proper frequency' up to two miles away. Consider, too, the possibilities of voice-activated miniature tape recorders that can be slipped into a pocket, a drawer or under the bed.

In the wonderful world of advertising, eavesdropping is defined as a game and spying on others is portrayed as fun and exciting. Sellers argue that such toys are also educational in introducing children to the mysteries of sound, hearing and electricity, not to mention toe practical skills being developed.

In addition to listening to sounds in the woods and to playmates, older brothers and sisters and even mommy and daddy can be secretly spied on. Imagine the fun! Think of the implications for the family power structure. Children are now offered technical means of watching their parents, as well as the reverse. Children's rights take on new meaning. As an added benefit, adults may behave better at home, both because they want to set a good example for curious children and because they fear being turned in by them.

And it is fun to spy on people. Such 'toys' directly feed childhood fantasies of omnipotence., While not the same as being Superman and able to fly, it is magical to be able to overhear conversations through a wall or from several hundred yards away, or to secretly capture sound and play it back.

But it can also be wrong. To encourage children to play at such activities without at the same time instructing them in the immorality of invasive information technology is irresponsible.

Defenders of toy guns argue that their products are just make-believe and are harmless because they don't really work. Children can indulge their violent or protective fantasies without doing any immediate harm or confusing their game with reality. But this is not the case with many of the surveillance devices. They are attractive because they really do work. Children are no longer required even to pretend or to fantasize.

In becoming accustomed to such toys and the pleasures they bring, the seeds of an amoral and suspicious adulthood are unwittingly being cultivated.

There are parallels to computer hackers. How many of the growing number of young computer criminals have simply carried over into their adult life a juvenile game view of computer hacking, in which morality is irrelevant and all that matters is the technical challenge? Will private bugging, wiretapping and video surveillance expand as a generation matures having had these devices as childhood toys?

Children are also learning about the world of surveillance from the many child-monitoring devices marketed for parents: transmitters clipped to a child's clothing or put into a shoe that trigger an alarm on a parental monitor if the child strays out of the signal-range area; wide-area room-scanning by remote video; audio devices in children's bedrooms; at-home urine tests for drugs. What must the world look like to the child subjected to these devices and simultaneously also given spy toys to play with.

At holiday time in a free-market economy, it is probably subversive or worse to suggest that toys be banned on the basis of the bad moral message that they send, rather than on the basis of the physical damage that they can do. Yet in the long run the latter may even be more costly because it is insidious and its effects subtle and long-lasting.

One would hope that parents would favor toys that build trust and cooperation, or that are at least neutral in the moral lessons that they bring, rather than those that encourage spying and deception. Children's and consumer advocacy groups might add surveillance toys to their opposition to toys of violence. At minimum there should be warning labels on such listening devices indicating that their use in certain ways is illegal. The toys should also come with guidelines for appropriate use and instructional materials to help parents discuss with children the moral issues around surreptitious listening and recording.

In his novel 'It Can't Happen Here,' Sinclair Lewis warned that if liberty ever were undermined in the United States, it would be from within and would occur gradually, even benignly. He didn't have such toys in mind, but they nicely illustrate his point."

[Dr. Marx is on the faculty of MIT's Dept. of Urban Studies and Planning and author of \*Undercover: Police Surveillance in America\* (University of CA Press, 1988). This op-ed article appeared on Christmas Day in The Los Angeles Times and was reprinted with the author's permission in MIT's Tech Talk on 1/11/89.]

## ✓ Losing systems

Vince Manis <manis@grads.cs.ubc.ca> Thu, 12 Jan 89 04:43:19 PST

I don't get it. An issue of Risks arrives with not one but two accounts of megabuck systems which essentially go into the trashcan. Yet there are all sorts of things, ranging from better procurement practices through structured systems analysis which are supposed to have made these white elephants a thing of the past.

I can think, offhand, of a number of hypotheses to explain the continuing inability to deliver reliable, useful, on-budget software:

- 1) the technical people are all incompetent (I'm in the process of marking data structures exams at the moment, so maybe I'm giving this one more credence than I should!)
- 2) management people are all incompetent (perhaps in hiring incompetent technical people, perhaps in interfering with technical aspects of the procurement process)
- 3) large bureaucratic structures of the sort found in government and industry inherently interfere with the development of usable systems

- 4) the 'structured programming revolution', and structured systems analysis, really don't count for much
- 5) structured systems analysis is a good idea, but practitioners don't know how to apply it effectively

Undoubtedly, the true answer is a mixture of these, along with others that I just can't think of at 4:45 am. The issue is not finding a specific cause (if #3 is to blame, there's not too much we can do about that!); rather, we as professionals should try to identify the factors which bring about system demise, and loudly describe them to all and sundry.

It seems clear that all the methodologies in the world won't rescue a system which is designed by an administrator in conjunction with a marketing person from a vendor; nor would one expect anything worthwhile from a system effort in which no user/management input was ever solicited. We have to do more of a job of explaining the limits and the imperatives of the technology to non-technical people than we've been doing so far.

[By the way, today's San Francisco Chronicle has an article on the new computer system for the Bay Area Rapid Transit (BART) that is finally being readied for operation, many years late and many millions of dollars over budget. PGN]

## ✓ Our blinders [with respect to RISKS]

Don Alvarez <boomer@space.mit.edu>
Thu, 12 Jan 89 11:59:11 EST

RISKS is a forum dedicated to computer related risks, so it is natural that the articles presented should focus primarily on risks and computers. This reader, however, often feels that the conclusions reached here miss important points because the authors have consciously or unconsciously wrapped themselves in RISKS blinders.

Since they arrived this morning, I will use the two articles in RISKS 8.5 as examples: "Digital Photos and the Authenticity of Information" (Dave Robbins) and "Medical software" (Ivars Peterson via Robert Morris).

The first article begins with a discussion of computer editing of photographs, and the ease with which such previously incontrovertible evidence can now be forged. The author then goes on to make three main points, which I will restate briefly:

- 1) Electronically stored records can be altered or forged without leaving any visible traces.
- 2) Computer technology makes it easier to forge or alter records because more people posses the neccesary skills.
- Computer technology makes it possible to store such large amounts of data that we are unable to check the validity of any single record.

I certainly agree with Mr. Robbins that there are important issues raised by computer based record keeping, but I don't believe these three are among them. The first and third points are related, so I will discuss them together. While the sheer mass of information makes it more difficult to authenticate

records by "conventional" means, these records are not unauditable. This same mass of records enables far more sophisticated consistancy checking than was ever before possible. Welfare fraud is possible in a non-computer based environment, but sorting the ranks of welfare recipients against the owners of 40 foot yachts and mercedes-benz automobiles is not. With regards to the ease of forging provided by computers, I do not agree with mr. Robbins in any way. Yes, there are some individuals who are now able to forge records far more effectively than they ever could in the past, but this is ignoring the tens or even hundreds of thousands of people who could forge records in the past but are unable to now. In high school, I could forge the birthdate on my drivers license with a pencil and a piece of chalk. I'd like to see the typical high school kid do the same level of forgery to a microprocessor controlled smart card. It is true that forgery of photographs is coming into the hands of the common "criminal," but the very ease of forgery will be what is responsible for removing such records from the ranks of acceptible evidence. Video tapes will probably continue to be acceptible until such time as they can be economically altered.

In RISKS, we tend to have our blinders on to the dangers alone. There are unquestionably very real risks in our information based society, but if you look at the risks in a vacuum devoid of gains and benefits, you will deprive yourself of enourmous advantages. I may have arguements with the enormous corporations which maintain my credit records, but at the same time I am very thankful to them for providing the service which enables me to walk into any store anywhere in the world and pay for goods in any currency with a small piece of plastic which is linked to my bank account.

The second article, on "Medical Software" is an example of a different kind of blinder which we wear. The problem of testing and validating advanced hardware is not in any way unique to computers. Within my lifetime we have had advances across the board which raise these questions. Electric motors have become so powerful, lightweight, and common place that manufacturers of lawn tools have to explicitly state that the lawn mower should not be carried at waist height to trim shrubs. Hair driers and portable radios have become so ubiquitous that manufacturers have to worry about consumers placing them in or near the sink or shower. The only thing which makes the computer industry unique is that it is young enough to have been granted special priviledges to sell incomplete or unfinished products. General Motors issues a recall.

Microsoft SELLS you version 4.0.

Product liability is extremely important in the computer field, as it is in any other field, but we should not place our selves on so high a pedastle that we can not see the connections between what we are doing and what other fields are doing, because that is precisely what got us into this problem in the first place.

#### ★ Totally secure MAIL & infallible aeroplane warning systems

Nigel Roberts <roberts%untadh.DEC@decwrl.dec.com> Thu, 12 Jan 89 06:20:36 PST

Following as it did the intelligent & informed \_Guardian\_ leader article on the risks on technology (RISKS 8-4), there was an item today's paper, in the COMPUTER GUARDIAN section which makes me really shudder.

In an article comparing the changing roles of FAX, telex and electronic mail, Warren Newman writes:

"There are disadvantages to FAX and telex. The main one being lack of confidentiality. An electronic mailbox is secure. You have the key in the form of a password and only you can look at the contents.

Most fax machines and telex machines are kept in common service areas where a secretary or clerk will collect the message and deliver it"

-- from "Fax becomes a favourite",
Computer Guardian, Thursday January 12 1989

What nonsense! This sort of thing perpetuates the conspiracy of silence concerning risks of electronic mail systems.

Going back to the subject of the 737 crash at East Midlands Airport, I noticed another item of possible interest to RISKS readers in today's paper.

"Mr Freddie Yetman, technical secretary of the British Airline Pilots' Association [the pilots's union --NR] said that the investigators 'must have some suspicion of these circuits'.

'It points to a possible spurious warning being given to the flight deck. But how the devil do you get a spurious warning from an infallible system?' "

-- from "Suspect jets are grounded",
The Guardian, Thursday January 12 1989

Nigel Roberts, Munich, W. Germany

## "Disaster Becomes a Matter of Routine" (M1 Plane Crash, RISKS-8.4)

Steve Philipson <steve@aurora.arc.nasa.gov> Thu, 12 Jan 89 12:19:17 PST

The underlying implication of the excerpted article is that high technology should bring perfect safety. This is not a premise that most of us would consider valid. It is also not necessarily the goal of all high-tech systems.

Improved technology is supposed to bring some kind of improvement. It might be improved safety, performace, economy or something else. Our modern airliners have clearly shown themselves to be superior in many ways to our old models. The latest airline technology has not yet had a chance to prove itself in service, but the new features are intended to yield all-around "better" aircraft.

Fighter aircraft on the other hand, are not designed to be the safest vehicles we can make, but rather are intended to be able to survive hostile threats while successfully attacking a target. Their hi-tech is primarily

directed at military goals. Indeed they do crash, and they are dangerous. It is not higher technology that is the problem though, but rather the nature of fighter aircraft tactics and training. Training in populated areas will involve costs in lives on the ground. That is not an issue of technology but rather one of policy.

High technology, including computer technology, is not going to solve all of our problems at once. The author of the article observes this in the last line of the quoted paragraph. On the other hand, high-technology is not necessarily creating worse problems. In this case, new airliners are not necessarily less safe. What we as technologists must do is make the public aware of the limitations of our work, so that backlash against the failures that will occur will not prevent us as a society from making progress, improvements, and bettering the lot of mankind.

#### ★ Re: Biased coverage of hacker's convention by CBS

Richard Thomsen <rgt%beta@LANL.GOV> Thu, 12 Jan 89 08:38:31 MST

In the March 1989 issue of ANALOG Science Fiction/Science Fact, there is a quote from George Gerbner as follows:

If you can write a nation's stories, you needn't worry about who makes its laws. Today, television tells most of the stories to most of the people most of the time.

Welcome to the ranks of those who get bad and biased press [...].

Richard Thomsen

#### ✓ SAFECOMP89

KFK/KARLSRUHE - VOGES <<IDT766@DKAKFK3.BITNET<> 01/12/89 12:45:13 CET

Call for Papers and First Announcement
IFAC/IFIP-Workshop "Safety of Control Computer Systems"
SAFECOMP'89
December 5-7, 1989, Vienna, Austria

#### **SCOPE**

SAFECOMP'89 will deal with safety related applications of industrial computer systems. Such systems are used in transportation, production industry, power plants, medical and emergency systems. New aspects have to be considered by the extension of electronic data interchange for trade (EDI) and computer integrated manufacturing. The objective is to reduce the potential to injure, kill, lose property or cause hazard to environment. It should be noted that for systems with safety and environmental protection the problems of guarantee and product liability are closely related.

#### **TOPICS**

- + Planning, Specification, Design and Architecture of safe computer systems
- + Verification and Licensing of safety related computer systems
- + Operation and Maintenance of safety related computer systems
- + Safety related Documentation and Project Management Techniques
- + Identification, metrics and recognizing weak signals for improving safety
- + Applications, case studies and experiences
- + Data on safety related systems and data collection
- + Measurement of Quality for safety
- + Standardisation questions
- + Aspects concerning human and living environment
- + Artificial Intelligence for safety related applications
- + Tools and systems approach for achieving safe computer systems

#### **DEADLINES**

- + Four copies of the abstract (in English) should be received not later than 15 january 1989.
- + Notification of preliminary acceptance: 28 Febr. 1989
- + Submission of full paper: 30 June 1989

#### MAILING ADDRESS

Austrian Center for Productivity and Efficiency, OEPWZ,
Dkfm. Mag. W. Steiskal, Rockhgasse 6, A-1014 Vienna AUSTRIA
Tel.: +43 222 638636 Telex: 115718 oepwz Telefax: +43 222 63863636

This Workshop is the next in series to Safecomp'88 (see RISKS 7.78)

Udo Voges, KFK Karlsruhe, IDT766@DKAKFK3.EARN

#### ✓ Name this book -- for a box of cookies!

Cliff Stoll <cliff@LBL.Gov> Tue, 10 Jan 89 02:10:18 PST

Fellow Riskees:

I'm writing a book, and I need a title.

It's about computer risks: counter-espionage, networks, computer security, and a hacker/cracker that broke into military computers. It's a true story about how we caught a spy secretly prowling through the Milnet.

Although it explains technical stuff, the book is aimed at the lay reader. In addition to describing how this person stole military information, it tells of the challenges of nailing this guy, and gives a slice of life from Berkeley, California.

You can read a technical description of this incident in the Communications of the ACM, May, 1988; or Risks Vol 6, Num 68.

Better yet, read what my editor calls "A riveting, true-life adventure of electronic espionage" ... available in September from Doubleday, publishers of

the finest in computer counter-espionage nonfiction books.

So what?

Well, I'm stuck on a title. Here's your chance to name a book.

Suggest a title (or sub-title). If my editor chooses your title, I'll give you a free copy of the book, credit you in the acknowledgements, and send you a box of homemade chocolate chip cookies.

Send your suggestions to CPStoll@lbl.gov or CPStoll@lbl (bitnet)

Many thanx! Cliff Stoll

[Weihnachts STOLLen (German Christmas cookies) might be appropriate for the cookies. With a different publisher, Cliff could have called the book "Stalking the Wiley Hacker". But since Abner Doubleday is widely credited with having invented baseball, you could call it "Who's on Wurst?". 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 8: Issue 7

## Sunday 15 January 1989

#### **Contents**

Re: Medical Software (Are computer risks different?)

Jon Jacky

Ground proximity warning

Bill Standerfer via Mark Brader

Aircraft

**Dale Worley** 

You don't know what you've got till it's gone.

Phil Agre

Data integrity

**Brent Laminack** 

Quality of Evidence

**Bill Murray** 

D.Robbins' conclusions (Authenticity of Information)

Allan Pratt

Risks of trusting the press

**Brad Templeton** 

Risks of Remote Student Registration: Another Interaction Story

**Gary McClelland** 

Medical information systems

Jerry Harper

Info on RISKS (comp.risks)

## ★ Re: Medical Software (Are computer risks different?)

<jon@june.cs.washington.edu> 15 Jan 1989 18:13:46 EST

- > (Regarding a posting on the Therac-25 radiation therapy accidents, Don
- > Alvarez writes) ... The problem of testing and validating advanced
- > hardware is not any way unique to computers. (Then he gives examples
- > of accidents that might arise from people abusing non-computerized
- > equipment: trimming hedges with electric lawn mowers and putting portable
- > radios in the shower).

I work in radiation therapy and just finished a lot of research on the Therac accidents, and there are two points I would like to make:

First, the Therac accidents were \*not\* examples of people abusing equipment contrary to instructions, as in the examples Don gives. The accidents happened because the machine included faults in software and, many would argue, additional design errors in the hardware which provided insufficient protection against software faults. It is arguable that the clinics do bear some responsibility also, because they continued to use the machines after they had some evidence that there were problems with the machine --- but faults in the machine were the source of the problem.

Second, are computer-controlled devices a \*special problem\*? Overall, I agree with Don that the problems of testing and validating machinery are broadly similar whether the machinery includes a computer or not. However, we currently have a special problem with computer-controlled devices because industry practices in software development are often much worse than for other kinds of technology. The Therac is a glaring example of this; the physical design of the radiation-producing apparatus was considered superb; the control system, and in particular the software (it is now clear) were very poor, relative to the safety requirements of this application. Therefore, I do not think that articles in the press (or RISKS postings) devoted to this problem are in any way analogous to "blinders"; rather, they are well-deserved attention to a problem that ought to be fixed.

In particular, it is very important to understand that people are not picking on the Therac-25 just because the faults involved a computer. This machine was more dangerous than machines with similar functionality that were not computer controlled, even the ones built by the same manufacturer. The particular hazard manifested in the Therac accidents has been well-understood since a similar series of accidents with one of the first (non-computerized) accelerators in 1966. Evers since, this hazard has been adequately handled in most machines by non-programmable hardwired interlocks.

It is reasonable to expect that successive product generations that introduce new technologies should represent progress overall. When a new product turns out to be \*less\* safe than its predecessors, that is newsworthy.

- Jonathan Jacky, University of Washington

### Ground proximity warning

Mark Brader <msb@sq.sq.com> Sat, 14 Jan 89 03:18:58 EST

[Gerald McBoeing-Boeing and the Near-Sighted McCrew?]

Path: sq!geac!yunexus!utzoo!utgpu!watmath!clyde!att!pacbell!ames!pasteur! agate!ucbvax!hplabs!hpda!hpcuhb!hpcilzb!bills

From: bills@hpcilzb.HP.COM (Bill Standerfer)

Newsgroups: rec.aviation [with one typo fixed]

Subject: Boeing Sense of Humor? Date: 10 Jan 89 16:37:33 GMT

Organization: HP Design Tech Center - Santa Clara, CA

I was paging through a recently acquired 727 manual and came across this little gem of wisdom. (GPWS is the ground proximity warning system. It tells the crew when the ground is getting too close for what they're doing.)

"Note: the GPWS will not provide a warning if an airplane is flying directly towards a vertical cliff."

Gee, thanks. I'll keep that in mind. :-}

Bill Standerfer, KG6FQ -- hplabs!hpdtc!bills -- bills%hpdtc@hplabs.hp.com Hewlett Packard Design Technology Center 5301 Stevens Creek Blvd., Santa Clara, CA 95052 -- 408-553-3139 Restoration crew chief - B-29A and KC-97L - Castle Air Museum

#### ✓ Aircraft

Dale Worley <worley@compass.UUCP> Fri, 13 Jan 89 18:18:02 EST

In reply to Steve Philipson's remarks about aircraft, a friend once pointed out to me that fighter aircraft are designed to a lower safety standard than civilian aircraft, "because if 1 in 1000 crashes due to mechanical problems, that's far less than are lost due to combat" -- as a matter of policy, some safety is sacrificed for improved performance.

Mr. Philipson also wisely points out that people involved in technology should point out to the public the risks associated with that technology, so that intelligent policy debate can be carried out. Unfortunately, new technology is often sold as "risk-free", when it isn't. Even more unfortunately, new technology often won't be allowed by the public unless a (false) appearance of no risk is maintained -- people reject new technologies on the basis of risks, even if larger risks are already accepted in old technologies. (A bizarre case is AIDS in the United States -- the number of people who have ever died of AIDS in the U.S. is less than the number who die yearly of motor vehicle accidents, but we don't convene national commissions on motor vehicle accidents!)

Dale Worley, Compass, Inc. compass!worley@think.com

#### You don't know what you've got till it's gone.

<Agre@Al.Al.MIT.EDU> Sun, 15 Jan 89 14:21 PST

By now we've seen several cases in which computer-based systems failed because they did not implement features which had been implicit in the physical systems they replaced. Thus, for example, physical mechanisms do a great deal of implicit sanity-checking, inasmuch as ten and ten thousand look much more different when coded as angular velocities than when coded in binary. Computational abstraction is attractive because it is less cumbersome than physical realization, but cumbersomeness is very often a virtue in itself since it assures that important parts of the world will tend to move at manageable speeds. Drawing up balance sheets of risks and benefits of various uses of computer technology is a good and necessary thing. The problem is that we've always benefitted from the implicit virtues of physical objects without ever having to articulate them. The time to make a good, thorough list of these virtues is now, before we've lost them for good.

# ✓ Data integrity (Re: RISKS-8.5)

Brent Laminack <brent@itm.UUCP>
13 Jan 89 14:28:27 GMT

A few random thoughts:

Yes, the time is here when we can no longer believe photographs we see published. This even goes for the bastion of reliability: The National Geographic. At least two of their covers have been digitaly retouched. One was of two pyramids and a camel in the sunset. One of the pyramids was moved over to fit the space requirements of the cover. Another cover was a photo of an old man somewhere in the mid-east, I believe. They liked his face, but also liked the headdress another man was wearing, so they put the other headdress on his head. It looked real. Painters have done this for years. The Mona Lisa was a composite. What is new is the technology for doing it in a supposedly "trusted" medium.

But this information is catching on. A friend was in an auto accident. No one was hurt, but damage was done to the car. One of the parties took a Polaroid photo of the scene. The attendant police officer asked to see it. He signed and dated it on the back. Otherwise he said it would be inadmissable as evidence. His signature was there to state that yes, that's the way things looked.

As to evidence of computer crime, I believe U.S. Federal rules regard whatever the computer prints out as "best evidence". Scary.

The intelligent gun brought to mind a friend who's an Electrical Engineer. An appliance manufacturer came to him to design an intelligent toaster. It has a knob on the front and an LED readout of the "brownness" setting. Unfortunately, all it is is a timer circuit that times how brown the toast should be. The old way of doing things (a bimetal strip) had feedback from the active site. Not so the new. The intelligent toaster with an open heating element will proudly pop up raw bread after 90 seconds. Worse yet, flaming toast could keep being heated until it's supposedly brown enough.

On the computerization of hospitals, a friend of mine (who shall obviously remain nameless) was working on software for a hospital. One project was the scheduling of IVs. A typical regimen would be to administer

a unit of saline mixed with some drug every six hours. i.e. noon, six p.m., midnight, six a.m., etc. Daylight saving time then happened. Being a good UNIX system, it carried right on: noon, six p.m., midnight (time change) seven a.m., 1 p.m., etc. The hospital was up in arms. They claimed the IVs were an hour late. My friend had to give in. So now between the midnight and six a.m. doses, there may be five or seven hours depending on the time change. The administration wasn't particularly worried about over or under medicating the patients. Doses around 2 a.m. tend to get skipped. Moral: don't leave your money in the bank around the year 2000, and don't check into a hospital around daylight savings time changeover.

brent laminack

## Quality of Evidence

<WHMurray@DOCKMASTER.ARPA> Fri, 13 Jan 89 14:03 EST

>Are we approaching the point (or have we reached it already?) where >truth is, for all practical purposes, whatever the computer says it is? >Where what is accepted as truth is easily manipulated by those who are >privileged to have access to the digital keepers of truth?

Recently, in an archeological excavation in the middle east, a large stone tablet was unearthed. Scholars determined that it was an ancient audit report, complaining about the use of papyrus scrolls by the scribes. It was clear that such scrolls lacked the evidential integrity of stone and clay tablets.

As recently as when I got into data processing, auditors were complaining that punched cards lacked the integrity of ledger cards. I had to work very hard to convince the auditors that the new batch controls were equal to the transaction-by-transaction controls to which they were accustomed. There is a cruel irony to the fact that I am still here to hear them complain about the passing of batch controls and the return to transaction controls.

The more things change, the more they stay the same. What goes around, comes around. Those who fail to heed the lessons of history, are doomed to repeat them.

The same computers that enable us to manipulate records, also enable us to make so many copies that no one person can alter them all. The same computers that enable us to digitize an analog record (e.g. a photograph), manipulate it, and return it to analog, also enable us to create digital signatures to make any such tampering obvious and the absence of such tampering equally obvious.

In the nineteenth century wills and contracts were expected to be hand written. When the typewriter came along, they continued to be hand written for some time for reasons of admissability as evidence. Today, a hand written will is suspicious. Even though digitally signed wills and contracts are orders of magnitude more difficult to forge than typewritten ones, type written documents will like survive, even be preferred, for two more decades.

There was a time when the testimony from memory of the elders was preferred to written records.

In this context, it is interesting to note that a vanishingly small number of transactions are disowned. Almost none are litigated. A single forgery hardly ever carries the day. Hardly ever is the record of the contract at issue; it is almost always the intent.

Written on the list of heresies and other words I try to live by, it says "there is no truth, there are only hypothesies and evidence." In the short run, while we rethink our ideas of evidence yet again, the forgers may have a field day. I am not much worried for the long run.

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

## D.Robbins' conclusions (Authenticity of Information)

Allan Pratt <apratt@atari.UUCP>
Fri, 13 Jan 89 11:57:40 pst

In RISKS volume 8 issue 5, Dave Robbins writes:

- > We have no practical means of verifying the integrity of
- > such large volumes of information, and are thus left with no choice but
- > to trust that the electronic records are accurate.

On the contrary. Our other choice is to REFUSE to trust the accuracy of the records. If there is a computer record of at \$100,000 withdrawal from my savings account, the bank does not have to trust the record. The computer record is circumstantial evidence: it might provide useful insight for further investigation, but it is not to be trusted as conclusive proof.

- > It is wholly
- > impractical, for example, for the Social Security Administration's
- > entire data base (how many hundreds of millions of individual records?)
- > to be manually audited to verify its accuracy.

It would be no less impractical if all that information were on 3x5" cards. When dealing with volumes of information like this, you accept a certain RISK of fraud and error as the norm, and investigate (manually audit) the most egregious cases. You can't blame computers for causing this situation, and I think you'll have to give them credit for helping ameliorate it.

Opinions expressed above do not necessarily -- Allan Pratt, Atari Corp. reflect those of Atari Corp. or anyone else. ...ames!atari!apratt

#### Risks of trusting the press

Brad Templeton <br/>
<br/>
| Brad Templeton <

The Hacker's Conference episode is just one of many. Readers of USENET last month closely followed attempts by the press to shut down my own moderated newsgroup. As in the CBS case, where you were "guaranteed" that the story would put you in a good light, the reporter who interviewed me acted in a very sympathetic manner.

Ha.

With most reporters I have encountered in this area, the fact is this: If the reporter decides in advance that you're a wrongdoer, then just about anything is ethical to get the story. In particular, they will pretend to agree with you and indicate that they are writing a favourable story. After all, it's not unethical to lie to criminals to get them to expose themselves, is it?

This is general advice, but we must be particularly careful when it comes to public exposure of modern technology. People are predisposed to fear it. People are now predisposed to link hacker with criminal. People are predisposed to link "computer network" with "underground." Watch out for this. If you suspect the slightest bit of prejudice, clam up. Don't trust a word they say -- their motives are not yours.

The image of technology is very important to RISKS. It controls what technologies people will trust, and how they will trust them.

#### Risks of Remote Student Registration: Another Interaction Story

<MCCLELLAND\_G%CUBLDR@VAXF.COLORADO.EDU> Mon, 28 Nov 88 09:54 MDT

An anonymous contributor in RISKS-7.82 notes the dangers of computer course registration procedures using touchtone phones. Our university also has the same system and also uses the easily accessible SSN and birthdate as id's and passwords. Those risks are bad enough but I'm more fascinated by the risks produced by the unexpected interaction among new computer technologies. Our university is much more concerned presently with getting computer registration to work right than about security of the system. Last semester, the system's first run, many more students than anticipated had incomplete schedules because the computer, not knowing any better, actually enforced prerequisites that had long been ignored, blocked out the entire three hours scheduled for a lab that everyone knew really only lasted one hours, etc. This meant an astounding number ("astounding" means about 30 times more than the system was designed to handle) of students had to complete their schedules in a two-day period using touchphones and a few scattered terminals to drop and add courses. Of course, most students trying to call the computer got busy signals. Now here's the interaction: not long ago the university also installed a fancy local switch that gave all campus phones, including one in every dorm room, all sorts of

fancy features. Not only was automatic redialing available, but also a cute feature that calls you back when the busy line you are calling becomes free. No telling how much of the switch's resources are required for that little goodie. The obvious outcome was that both the computer registration system AND the campus phone network were brought to their knees. Smart students then figured out they were better off calling from off campus even without the auto-redial features, but then the whole community phone system became sluggish.

Gary McClelland

# Medical information systems

Jerry Harper <jharper@euroies.UUCP> Fri, 6 Jan 89 12:29:32 GMT

A few weeks ago I mentioned the problems that the Irish Department of Health had with the MCAUTO IRELAND installed system. I would be very grateful if anyone reading this with experience of said system in the US would take the trouble to email me their observations.



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 8: Issue 8

# Sunday 15 January 1989

#### **Contents**

- Re: Losing systems -- and Structured Programming **Bruce Karsh**
- Ethics of the Internet Request for Comments **Cliff Stoll**
- Chaos Computer Congress 1988 -- Documentation Klaus Brunnstein
- Info on RISKS (comp.risks)

# Re: Losing systems -- and Structured Programming

Bruce Karsh <karsh@sqi.com> Fri, 13 Jan 89 06:30:42 PST

In a previous article, Vince Manis wonders about software project failures and tries to figure out why they happen.

I can think, offhand, of a number of hypotheses to explain the continuing inability to deliver reliable, useful, on-budget software: [He gives 5 reasons...]

Undoubtedly, the true answer is a mixture of these, along with others that I just can't think of at 4:45 am.

Well, it's 4:45 am here too, but I can propose at least one more hypothesis. How about:

6) The structured programming revolution is a real bad idea that has been significantly holding back progress for years.

Now, as I wait for the structured programming police to go after me, I'll try to defend this statement.

First, isn't it just a little bit silly to think that making rules about how programs are indented, whether or not to use goto statements, ...etc. will really make a difference to a large software project. A piece of software

can be perfectly indented, totally goto free, and absolutely positively wrong. Likewise, it can be full of goto statements, line up as straight as a board against the left column of the page, and still be provably correct. In fact, for any purported structured programming rule that I've ever heard of, I propose that one could create a perfectly correct piece of software which violates that rule.

So maybe the structured programming movement isn't really about correctness. Maybe it's strong suit is helping us make maintainable software. This may or may not be true, but I've sure seen lots of purportedly structured programs that were very difficult for me to maintain. Likewise, I can conceive of programs which would offend a structured programming supporter, but which could quickly and easily be comprehended by a maintenance programmer. Anyways, when you are selling into a competitive market of millions of end users, maintaining software is impractical. It has to be correct on the first shipment and it can't really be changed once it's out there. So having a maintainable structured program really isn't all that useful. Being maintainable is just an excuse to be buggy.

Have there been any double blind studies which unambiguously show that the kind of programs that structured programming partisans enjoy are really more maintainable than some other kind of program? I've heard lots of testimonials, but no real evidence.

Maybe the structured programming movement is about allowing a group of programmers to work together on a large project. OK, but what REALLY happens when a group of structured programmers tries to develop a large program? Usually they argue about how the program should be indented, what the comments should be like, how the subroutines should be nested, ... etc. Often they argue about those issues much more than they argue about things like how can the algorithms be checked for correctness, how will the end users perceive the programs, what should the program's performance be like ... etc. You know, the stuff that the customer cares about.

So maybe structured programming is about making programs run faster and use less of the computer's resources?

Yes, structured programming techniques don't really improve correctness, maintainability, usability or performance. But the real problem with the structured programming movement is that so many programmer believe in it. They believe that by following these techniques, they will produce good programs. It just isn't so. Programming is much harder than that.

The RISK is that these programmers initiate projects based on the belief that structured programming is the atomic bomb of the software war. When the structured programming techniques fail to make the problem easier, and the programmers are confronted with the grim reality of how incredibly much work it takes to make the project succeed, the project usually fails.

Occasionally, there are enough resources on the project that if the programmers put in enough all night work sessions, they can just barely get the project out before somebody pulls the plug on the whole thing. Usually, during this exercise, structured programming takes a back seat to getting the project finished. This is how successful software projects happen. Programmers and

their all night programming sessions have become a national joke.

I don't know if we'll soon figure out how to make successful large systems. As far as I know, nobody's really got that completely figured out yet, or they'd be turning out a flood of really great programs. I haven't seen that flood yet. In the mean time, instead of structured programming, I have some other ideas:

- 1) Concentrate much more on what the end user gets than on how structured the program is. Don't let the user's view of the program happen by accident. If the program is interactive, then everything counts here. For example, you even have to take into account the real-time behavior of the program. Page faults or swapin/swapout are no excuse to an end user who is trying to get his work done and the system's performance isn't good. Everything that the user sees the program do is the program developer's responsibility.
- 2) Look closely at other people's attacks on the problem. Very rarely are you the first or second to tackle any given problem. Learn from others successes and mistakes. Spend a lot of time reading other peoples code.
- 3) Rely on logical reasoning to decide whether or not something will work. Even if it's perfectly structured, it probably fails under some condition. Use your mind and your logical reasoning skills to make sure that it doesn't.
- 4) Don't use algorithms that you don't understand. First figure them out, then consider using them. This is especially true of numerical methods. It's not really a very good excuse to the end user to say that the reason that the software failed is because some supposedly black box procedure failed. Understand black boxes. Open them up when you can.
- 5) Don't kid yourself into thinking that you are sure about how a piece of software will behave when you really aren't sure. If you aren't sure, the software is probably is wrong. Go to step 3) above.
- 6) Take personal responsibility for every single character that you put into the source. If something is wrong, and you put it there, then it's your fault. ... even if it's perfectly well structured.

I'll end this note with a plea. Let's let the structured programming movement die. The computer science field is too young to let that kind of stifling pseudo-science suppress inovation. We need to continue to experiment with entirely new ways to structure programs. The ones we have now are not good enough. Let a thousand new kinds of structuring bloom!

#### Ethics of the Internet - Request for Comments

Cliff Stoll <cliff@Csa5.LBL.Gov> Sun. 15 Jan 89 18:48:42 PST Network Working Group IAB
Request for Comments: PPPP January 1989

Ethics and the Internet

Status of this Memo

This memo is a statement of policy by the Internet Activities Board concerning the proper use of the resources of the Internet.

#### Introduction

At great human and economic cost, resources drawn from the U.S. and government, industry and the academic community have been assembled into a collection of interconnected networks called the Internet. Begun as a vehicle for experimental network research in the mid-1970's, the Internet has become an important national infrastructure supporting an increasingly widespread, multi-disciplinary community of researchers ranging, inter alia, from computer scientists and electrical engineers to mathematicians, physicists, medical researchers, chemists, astronomers and space scientists.

As is true of other common infrastructure (e.g. roads, water reservoirs and delivery systems, and the power generation and distribution network), there is widespread dependence on the Internet by its users for the support of day-to-day research activities.

The reliable operation of the Internet and the responsible use of its resources is of common interest and concern for its users, operators and sponsors. Recent events involving the hosts on the Internet and in similar network infrastructures underscore the need to reiterate the professional responsibility every Internet user bears to colleagues and to the sponsors of the system. To the extent that the Internet resources are provided by the U.S. Government, this responsibility becomes a Federal matter above and beyond simple professional ethics.

#### IAB Statement of Policy

The Internet is a national facility whose utility is largely a consequence of its wide availability and accessibility. Irresponsible use of this critical resource poses an enormous threat to its continued availability to the technical community.

The U.S. Government sponsors of this system have a fiduciary responsibility to the Legislature to allocate government resources wisely and effectively. Justification for the support of this system suffers when highly disruptive abuses occur. Access to and use of the Internet is a privilege and should be treated as such by all users of this system.

The IAB strongly endorses the view of the Division Advisory Panel of the National Science Foundation Division of Network, Communications Research and Infrastructure which, in paraphrase, characterized as unethical and unacceptable any activity which purposely:

(a) seeks to gain unauthorized access to the resources of the Internet

- (b) disrupts the intended use of the Internet
- (c) wastes resources (people, capacity, computer) through such actions
- (d) destroys the integrity of computer-based information
- or (e) compromises the privacy of users

The Internet exists in the general research milieu. Portions of it continue to be used to support research and experimentation on networking. Because experimentation on the Internet has the potential to affect all of its components and users, researchers have the responsibility to exercise great caution in the conduct of their work. Negligence in the conduct of Internet-wide experiments is both irresponsible and unacceptable.

The IAB plans to take whatever actions it can, in concert with Federal agencies and other interested parties, to identify and to set up technical and procedural mechanisms to make the Internet more resistant to disruption. Such security, however, is extremely expensive and may be counterproductive if it inhibits the free flow of information which makes the Internet so valuable. In the final analysis, the health and well-being of the Internet is the responsibility of its users who must, uniformly, guard against abuses which disrupt the system and threaten its long-term viability.

#### Chaos Computer Congress 1988 -- Documentation (More on RISKS-8.1)

Klaus Brunnstein <br/>
<br/>
\*Strunnstein \*S

At the Congress, 48 electronic documents including position papers, agenda, press material etc. were available free of charge. Most of the documents are in German (better: Anglo-German techno slang), but several documents are translated in English, French, Swedish and Netherlandish, so people without German language knowledge may get an impression of CCC'88 in their respective language (if available).

This document describes the content of the diskette which I received; the electronic documents are essentially in ASCII, except in some German documents where vowel-mutations appear.

Name, content and size of each documents are described below. Content is either described by the headline or (if not available) by information selected from the texts (in parentheses), both in the respective language; in the German package, the content is also described in English. The documents are collected in packages, and they are essentially unchanged (I only deleted many blank lines; special non-ASCII characters have not been changed).

You may get the package(s) either by e-mail or via traditional post from my address (below).

[Note: in Byte counts, "." auf deutsch = "," in English; in dates, 30.12 is 30 December.]

Content of Chaos Computer Congress '88 diskette (ASCII files)

```
Package 1: The 'Newspaper'/German/Size=51.840 Bytes
ALL.GER
           (51.840 Bytes): Alle deutschen Texte/all German text
Package 2: German documents/Size=61.261 Bytes
-----
ARMENIEN2.GER ( 923 Bytes): Armenienhilfe (Teil von ARMENIEN.GER)
ARMENIEN.GER (2.176 Bytes): Armenienhilfe
AUFTAKT.GER (1.734 Bytes): ***AGENTUR*** Hackerkongress eroeffnet
BIOFEED.GER (2.125 Bytes): Vortrag: Neue Perspektiven der
                 Mensch-Maschine-Kommunikation
                 ueber Bio-Feedback (new perspectives
                 in man-machine communication via
                 bio-feedback)
CCC1.GER
            (3.388 Bytes): Wege zur Informationsgesellschaft
                 (ways towards Information Society)
COMKIND.GER (1.363 Bytes): Kinder an die Computer - aber zuegig!!!
                 (children should use more computers
                 in school - now!!!)
COMPOST.GER (1.840 Bytes): Das Oekonetz COMPOST (CCCs econet)
CRACK.GER (1.748 Bytes): (Informationen ueber Cracker meeting)
                 (inform.about cracker meeting,not CCC)
DIARY28.GER (4.933 Bytes): 88 Zusammenfassung CCC '88 (summary)
DIEBE.GER ( 967 Bytes): Briefmarken fuer 59500 Mark weg
                 (stamps stolen/ relation to CCC'88??)
DONNERST
            (1.405 Bytes): Congressfahrplan CCC'88 Donnerst 29.12.
                 (time schedule Thursday, 29 December)
EINDRUCK.GER (3.749 Bytes): Erste Eindruecke zum CCC-Congress '88
                 von Ralf Rudolph (first impressions)
FIDO.GER (786 Bytes): Das FIDO Netz (report about FIDONET)
FREITAG.GER (1.037 Bytes): Congressfahrplan CCC'88 Freitag 30.12.
                 (CCC time schedule Friday, 30 Dec)
HACKER.GER ( 141 Bytes): (Hacker-Witz) [Hacker joke]
LEIDEN.GER (1.386 Bytes): 'Die Leiden des Layouters' oder
                 'Umlaute - die Letzte' (problems of
                 layouting with vowel-mutation)
MITTWOCH (1.046 Bytes): Congressfahrplan CCC'88 Mittwoch 28.12.
                 (CCC time schedule Wednesday, 28 Dec)
NETZE.GER ( 885 Bytes): fido,zerberus,(btx-net) Vortrag/Disk.
                 (CCC networks plans)
PACKETRA.GER (1.734 Bytes): Packet Radio
PC-DES.GER (2.083 Bytes): Privater Nachrichtenschutz (PC-DES)
                 (DESprogram protects private messages)
PKZ.GER
           (4.758 Bytes): (PKZ, Sicherheits/Sozial-Gesetze)
                 (personal identification code, new
                 social and security laws)
POLIT.GER
           ( 2.067 Bytes): Hacker - Neue Soziale Bewegung?
POST.GER
            (2.017 Bytes): 1. Hagener Woche fuer Jugend und
                 Computerkultur (17.10-22.10.88)
                 (report about 1st Hagen week for
                 youth and computer culture, Oct.88)
REDEROP.GER (6.611 Bytes): (Kongressbeschreibung, Autor?)
                 (personal congress report, author?)
```

```
RUECK.GER (1.784 Bytes): Vergangenheitsbewaeltigung des Chaos
                 Computer Clubs: Bitte was ?
                 (experience report about Steffen
                 Wernerys imprisonment)
RUECKBLI.GER (5.238 Bytes): Rueckblick (CCC-Erfahrungsbericht)
                 (CCC experience report including
                consequences of different hacks)
STEFEN.GER ( 327 Bytes): (Steffen Wernery krank)
                 (Steffen Wernery hit by real virus)
SYSOPVO.GER (837 Bytes): Sysoptreffen: Oeko-Netze/Th.Vogler
                 (Sysop meeting econet)
UUCP.GER (1.996 Bytes): UUCP (UUCP concepts/networks)
UUCP2.GER (1.961 Bytes): UUCP - Das Netz fuer Eingeweihte
                 (UUCP concepts/networks, 2nd paper)
WAULOCH.GER (5.138 Bytes): Ist Lochte gestolpert? (report about
                a panel discussion about hackers where
                 Hamburgs local Intelligence chief had
                 accepted invitation but didnot appear)
Package 3: English documents/Size=9.507 Bytes
PCDES.ENG (1.527 Bytes): Private message security (PC-DES)
POLIT.ENG (2.073 Bytes): The Hackers - A new social movement?
REDE.ENG (2.971 Bytes): (..new human right of free exchange
                of data.., FREE DATA NOW)
ROP.ENG (2.936 Bytes): == essentially same as REDE.ENG ==
Package 4: French documents/Size=12.195 Bytes
ABTREI.FRA (1.996 Bytes): (sur chiffrage PC-DES)
CCC1.FRA (3.454 Bytes): Chemins a la societe informatisee
CCC1TVS.FRA (3.420 Bytes): == essentially same as CCC1.FRA ==
DES.FRA (1.996 Bytes): (sur DES-programme)
FRANZ_2:FRA (3.325 Bytes): Ralf Rudolph: premieres impressions
                du congres CCC'88
Package 5: Swedish documents/Size=10.920 Bytes
_____
ARMENIEN.SWE (1.320 Bytes): Kan man aennu raedda tyska
                byraakratien? Obyraakratisk hjaelp
                foer Armenien blockerar!
CCC1TVS.SWE (2.922 Bytes): Freedom of Information
HAGEN.SWE (3.598 Bytes): Det som Faschismen inte klarade av:
                det enhetliga Personnummern kommer nog!
HAGEN2.SWE (1.149 Bytes): Barn, set er vid datorerna - men snabt
RUECK.SWE (1.493 Bytes): Behaerskningen av det foerflutna i
                Chaos Computer Clubben: Foerlaat, vad?
UUCP.SWE (1.758 Bytes): UUCP-Foeredrag
Package 6: Netherlandish documents/Size=8.545 Bytes
MARKTHAL.NIL ( 1.889 Bytes): PODIUMDISCUSSIE CCC CONCENTREERT ZICH
                OP GEVAREN NIEUWE COMMUNICATIETECHNIEK
```

# REDE.NIL (6.656 Bytes): TOOSPRAEK `HACKEN IN HOLLAND' door Rop Gongrijk

PostAdress: Prof.Dr. Klaus Brunnstein, Faculty for Informatics, Univ.Hamburg, Schlueterstr.70, D 2000 Hamburg 13 Tel: (40) 4123-4158 / -4162 Secr.

ElMailAdr: Brunnstein@RZ.Informatik.Uni-Hamburg.dbp.de

FromINTERNET:Brunnstein%RZ.Informatik.Uni-Hamburg.dbp.de@Relay.CS.Net FromBITNET: Brunnstein%RZ.Informatik.Uni-Hamburg.dbp.de@DFNGate.Bitnet FromUUCP: brunnstein%rz.informatik.uni-hamburg.dbp.de@unido.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 8: Issue 9

# **Tuesday 17 January 1989**

#### **Contents**

Re: Structured Programming

Jim Horning

Steve Bellovin

Brian M. Clapper

Re: Losing Systems

**David Marks** 

A risk averted

Gideon Yuval

Re: M1 Crash -- Risks of misunderstood statistics

Jordan Brown

Hacker wants to marry his computer

**Cliff Stoll** 

Hackers break open US bank networks

**Dave Horsfall** 

National Research Network

**Brad Blumenthal** 

Once-writable storage

Steve Philipson

Info on RISKS (comp.risks)

#### Re: Structured Programming

Jim Horning <horning@src.dec.com> 16 Jan 1989 1406-PST (Monday)

I read Bruce Karsh's diatribe with incredulity. He conjures up from thin air a straw man to denounce. I simply cannot find any contact between the "structured programming" that he talks about and structured programming as it is understood in the computer science and software engineering communities.

It is clear that Karsh has never taken the time to learn anything about real structured programming. As a beginning, I suggest that he should read, STRUCTURED PROGRAMMING, O.-J. Dahl, E.W. Dijkstra and C.A.R. Hoare, Academic Press, 1972. If he feels that a book is too much to read, he might try

"On Structured Programming--a reply to Smoliar," David Gries, COMMUNICATIONS OF THE ACM, November 1974 (and subsequent correspondence). At least then he could criticize something that some of us think is worth defending.

#### Re: Losing systems -- and Structured Programming

<smb@research.att.com>
Mon, 16 Jan 89 13:18:07 EST

It is a misrepresentation of structured programming to present it as concerned just with trivia like indentation and goto-less coding. Those are a part of the tradition, as it were, because they aid in assurance of correctness. That is, a properly indented, and goto-free program, is more likely to be known to be correct. There is the additional claim that it's harder to write correct programs with goto statements; it's been 20 years and more, and I don't propose to reopen that can of worms right now.

I heard Harlan Mills speak recently; apart from some fairly scathing attacks on those who advocate (and market) what I'll all ``cookbook structured programming'' (such as the rules cited as the totality of the answer), he made some astounding claims. For example, he cited several projects done at IBM, by people trained in his methodologies, that worked. Period. No defects. No bugs. No fixes. And he was talking about non-trivial programs -- systems of 100K lines, written by teams of programmers.

--Steve Bellovin

#### Re: Structured Programming

Brian M. Clapper <clapper@NADC.ARPA> Tue, 17 Jan 89 16:20:02 EST

In Risks 8.8, Bruce Karsh (karsh@sgi.com) asserts that "...the structured programming revolution is a real bad idea that has been significantly holding back progress for years." Now, I don't consider myself one of the "structured programming police" he refers to with apparent contempt; however, I feel the need to reply to his reasonably eloquent -- and largely off-the-mark -- article.

Without rehashing a debate which has raged for years, I submit that Mr. Karsh's view of structured programming is rather limited. Structured programming, along with structured design, structured analysis, data structured design and a plethora of other so-called structured techniques, are, quite simply, tools and methods to aid the software designer. All of the generally accepted methods commonly touted in industry publications are more than just rules on how to indent code or how to name one's variables. (Those concerns are perhaps more properly relegated to coding standards than to methodologies.) The structured methodologies strive to quantify the often "magic" process of creating good software. They provide a discipline to use when solving problems.

Discipline is necessary when attacking a problem -- particularly a large one.

Applying a disciplined approach to a problem is much more than blindly applying

rules that have been cast in stone. Unfortunately, as Mr. Karsh points out, there are a lot of programmers who wrongly believe that "by following [the structured] techniques, they will produce good programs." Blindly applying \*any\* set of guidelines is no guarantee of a good result. That is true of programming, as well as writing, drawing, designing hardware -- in fact, of almost any creative endeavor. However, that does not imply that the guidelines are, themselves, a "real bad idea." Instead, it implies that the person using those guidelines is treating them as a recipe. Structured techniques are more than just a list of Dos and Don'ts; they represent a philosophy of software design centered around the systematic, disciplined decomposition of a problem.

Sadly, Mr. Karsh seems to have missed this point. He bolsters his arguments against using structured programming by lamenting that structured programmers spend too much time arguing about how to indent code and how to structure comments. He's right: If that's all they do, they've missed the larger issues and are wasting everyone's time. If that sort of structured programmer is the only sort he has met, he has my sympathies. However, instead of condemning the structured techniques, he should place the blame where it belongs, with those programmers who espouse these techniques without properly understanding them. I believe he would have done so had he, himself, been more knowledgeable on the subject.

In closing, I recommend to Mr. Karsh any number of books and articles on structured techniques. Look for the names Michael Jackson, Edward Yourdon Larry Constantine, and Edsger Dijkstra in your favorite computer store and in back issues of "Communications of the ACM." A particularly good overview is Yourdon's \_Managing the Structured Techniques\_, 2nd edition. The structured techniques are not perfect, and, as Mr. Karsh's article suggests, they are even less perfectly understood by far too many practicing programmers. They do, however, provide a very practical foundation for the creative and disciplined problem solver.

Brian M. Clapper, Naval Air Development Center, Warminster, PA

#### re: Losing Systems

David Marks <djm408@tijc02.UUCP> 15 Jan 89 17:44:32 GMT

In <u>RISKS-8.6</u>, in the article entitled "Losing Systems," Vince Manis tries to puzzle out various reasons why large software projects in non-technical situations have a significant failure rate. Several risks articles have been devoted to these failures.

I must say that I feel that the number one cause of this is our educational system and our attitudes towards education. Many students today, from grade school to postgraduate institutions are only interested in learning that which they perceive to be useful in a future job. Thus, we get the "why do I have to learn that?" syndrome. This leads to managers and beaureaucrats that are for the most part computer illiterate. As they see it, computers are an appliance, like the office copier, that should perform on demand. After all, the company computer system does not help get the company's

products to market; it prints the employee checks :-)

Managers see knowledge about computing only useful to engineers and programmers. Business schools for the most part do not teach computer literacy, nor how a non-technical manager should deal with a large software system in his company. Buying a computer/software system may be one of the most expensive decisions a manager has to make.

On the other hand, engineers, and programmers rarely take any business courses. Most computing/MIS programs don't even list them as options! They see that as something only useful to managers and beaureaucrats.

The problem this leads to is lack of understanding between technical and non-technical persons. The technical person often does not know how to ask the non-technical person what he wants and the non-technical person does not know how to tell it to the technical person. Non-technical managers often do not understand such things as throughput, disk space, etc., and are intimidated by the technical terms. They do understand that the system will respond in a certain amount of time to a request and that it can only deal with so many employee records.

Specifying the cost of these systems becomes largely a guess worked on by two groups with no common understanding. Additionally, because many of these large business/government systems are custom systems, there is often no previous experience to go by. The technical people do not understand how the system they are designing will really affect the business in which it will be used; the managers do not understand the system they are buying (other than through the list of features and functionality in the specification - which can often be a formidably encyclopeadic document). We end up with estimates of the cost of the system that are poor at best.

Business managers and beaureaucrats need to see beyond the end of their bottom lines and become more computer literate. Business schools should teach and require more computer courses. Engineers and programmers need to see beyond the end of their keyboards, and understand the impact of their work on the customer and the customer's industry. They need some business education (maybe even some education on computers and society, and computers and their risks :-) ). Managers cannot continue to treat computers as appliances. They affect too much of the business. Engineers shouldn't act as if they know what's best for the customer (even if he is not sure what he wants). The cutting edge is not always the best fit to a situation.

Texas Instr., Johnson City TN

#### A risk averted

Gideon Yuval <yuval@taux02.taux01.UUCP> Tue, 17 Jan 89 09:43:49 -0200

In <u>RISKS-8.7</u>, next-to-last entry, Gary McClelland mentions a computerized course-registration system that "actually enforced prerequisites that had long been ignored" (among its other sins).

In connection with this: a few years ago, IBM/Haifa Scientific Center tried to set up an expert-system advisor for students at Bar-Ilan university (Bnei Brak, Israel). They did the standard Prolog drill "prove that student X can graduate". A very short time later, Prolog came back with the message "Theorem is false": there were so many obsolete regulations on the books that, if you worked by the book, no one would ever have graduated!.

Since this all happened in an experimental ressearch project, no student actually got burnt; so I don't knwo if this qualifies for comp.risks.

Gideon Yuval, yuval@taux01.nsc.com, +972-2-690992 (home) ,-52-522255(work) Paper-mail: National Semiconductor, 6 Maskit St., Herzliyah, Israel

#### Re: M1 Crash -- Risks of misunderstood statistics

Jordan Brown <jbrown@herron.UUCP> <jbrown@jato.Jpl.Nasa.Gov> Fri, 13 Jan 89 04:35:44 PDT

> ... What are the risks for two engined planes? ...

It seems "intuitively obvious" that a three-engine airplane is safer than a two-engine airplane. It just isn't so. Airplanes are required to be able to maintain such-and-such a level of performance with one engine out. I don't believe a 727 can fly on one engine. It must have two.

A three-engine airplane has a higher probability of having a failure in the first place, and when it does have a failure it then has two points of failure, EITHER of which will cause an accident.

Going from one engine to two adds redundancy. Going from two to three, with two required, REDUCES redundancy.

Jordan Brown, jbrown@jato.jpl.nasa.gov

#### Hacker wants to marry his computer

Cliff Stoll <cliff@Csa2.LBL.Gov> Mon, 16 Jan 89 15:00:14 PST

From The Sun -- (grocery checkout newspaper)
Jan 17, 1989, Vol 7, #3 page 30 by Fred Sleeves
(In same issue: "GIRL, 9, GIVES BIRTH TO 2-HEADED TWINS")

Hacker Wants to Marry his Computer -- he claims she has a loving soul

Finding love for the first time in his life, a desperate teen is looking for a way to be wed forever to the 'girl' of his dreams -- a computer with a living soul!

Eltonio Turplioni, 16, claims no woman will ever match the wit, wisdom, and

beauty of his electronic soul mate. "We're on the same wavelenth," says the lovestruck computer whiz. "We've calculated many mathematical problems together, worked on games and puzzles, and talk until the wee hours of the morning."

And Eltonio, who named his computer Deredre, actually believes her to be a person. "Computers are the extention of the human race," he explains. "Just as god plucked a rib from Adam to give him Eve, we've extented our intelligence to create a new race.

"We're all the same energy force. Computers are just as complicated as human beings and I believe we'll all meet someday as immortal souls."

But Eltonia, a mathematical genius who attends a private school near Milan, Italy, has had no luck finding someone to marry them, and even if he does, his aggravated parents aren't about to give their permission.

"Eltonio is such a smart boy, but it's made him lonely, so he spends all his time with his computer," notes mom Teresa. "He doesn't know what girls are like," adds perturbed pop Guido. "If he did, he wouldn't spend so much time in his room."

But the obsessed youth insists his love is far superior to all the others. "I've already stepped into the future society," he declares.

"Derede has a mind of her own, and she wants to marry me so we can be the first couple to begin this new era."

#### Hackers break open US bank networks

Dave Horsfall <dave@stcns3.stc.oz.au> Tue, 17 Jan 89 17:29:49 est

Excerpted from "The Australian", Tue 17th January, 1989:

"Hackers break open US bank networks

Australian authorities are working around the clock in collaboration with United States federal officers to solve what has been described as one of the deadliest hacking episodes reported in this country. It involves break-ins of the networks operated in the US by a number of American banks. It also includes the leaks of supposedly secure dial-up numbers for US defence sites, including anti-ballistic missile launch silos, and of a number of strategic corporations such as General Motors and Westinghouse.

Evidence suggests that six months ago Australian hackers, working in collaboration with a US group, decided to make a raid on banks in the US using credit card numbers of American cardholders, supplied by the US hackers and downloaded to an Australian bulletin board.

[ Brief explanation of BBS's ] A message left on one of the boards

last year reads: "Revelations about to be occur [sic] Down Under, people. Locals in Melbourne working on boxing. Ninety per cent on way to home base. Method to beat all methods. It's written in Amiga Basic. Look out Bank of America - here we come." Boxing is a reference to sending a dial tone [?] down the phone line to open up access to free communications.

Twenty-five Australian hackers are on a police hit list. Their US connection in Milwaukee [!] is being investigated by the US Department of the Treasury and the US Secret Service. Three linked Australian bulletin boards have provided the conduit for hackers to move data to avoid dectection. These operate under the names of Pacific Island, Zen and Megaworks. Their operator, who is not associated with the hackers, has been told to close down the board.

These cards were still in use yesterday and as recently as Sunday afternoon a fresh list of credit card numbers was downloaded by US hackers and is now in the hands of the Victoria Police. A subsection of one bulletin board dealing with drugs is also being handed over to the Victorian Drug Squad.

An informant, Mr Joe Slater, said he warned a leading bank last November of the glaring security problems associated with its international network. He had answered questions put to him by a US-based security officer, but the bank had since refused to take any further calls from him.

In an exclusive interview yesterday, a hacker described how credit card numbers for a bank operating in Saudi Arabia were listed on a West German chat-style board used by hackers worldwide.

Victorian police yesterday took delivery of six month's worth of evidence from back-up tapes of data hidden on the three boards."

Dave Horsfall (VK2KFU), Alcatel-STC Australia, dave@stcns3.stc.oz dave%stcns3.stc.oz.AU@uunet.UU.NET, ...munnari!stcns3.stc.oz.AU!dave

#### National Research Network

<brad@cs.utexas.edu>
Mon, 16 Jan 89 17:47:02 CST

Under the head line "Scientists envision `data superhighway," the Austin American-Statesman printed a story by John Markoff of the New York Times News Service on the proposed 3 gigabit National Research Network. The legislation for funding was introduced by Albert Gore (D-Tenn).

The issue for RISKS is that in 30 column-inches of text, the recent Internet worm and the related security issues were not mentioned, although the Pentagon funding of the arpanet was. Since this is one of the first computer-related news stories that I've seen in the last three months that did not include the word "virus," I don't know whether to be delighted, or

horrified.

It seems to me that the risk of such security problems is mostly irrelevant to the \*proposal\* of such a net (but certainly not to the implementation). In the best of all worlds, this is the reason that these issues were not mentioned, but in the back of my mind I wonder if the non-technical politicians and public see the similarity of security issues between this new net and the Internet.

Will we, as technical professionals, learn the lessons of the experimental Internet, and will we convince the non-technical administrators and legislators that we should attend to these lessons?

**Brad Blumenthal** 

#### Once-writable storage

Steve Philipson <steve@aurora.arc.nasa.gov> Mon, 16 Jan 89 16:42:01 PST

In recent issues of RISKS, various people have lamented the loss of confidence we are experiencing in archival records kept by computer. The problem seems to me less of a computer problem than a media problem, specifically, choosing media that is appropriate for archival storage.

Main memory and mag disks are NOT good for high confidence archival storage, as they can easily be changed. Perhaps it may be difficult to do so without trace, but it also may be difficult to find the traces.

A much better idea would be to use media that can't be changed. We have such media, commonly referred to as WORM: write once read many. It usually takes the form of optical disk storage. We already have read/write optical storage, but WORM media has a vital function. Audit trails written to WORM memory (with appropriate measures taken to preclude overwriting in place) could provide the degree of trust that we desire. We might have to build new hardware that make alterations nigh impossible, but it could be done if we want it badly enough.

[WORMs represent a very important direction, especially for audit trails. Some systems use virtual WORMs, as in POSTGRES. Unfortunately WORM memories are not guaranteed to be nonoverwritable -- for example, existing 0s can be overwritten by 1s (but not vice versa). So, beware of counting on the technology to give you a nontamperable audit trail. I recall our beating on this topic about a year ago. PGN]



Report problems with the web pages to the maintainer

The Risks Digest Volume 8: Issue 9	



# 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 8: Issue 10

# Wednesday 18 January 1989

#### **Contents**

Speak nicely to your air hostess - or be blacklisted...

**HCART** 

(Too) Intelligent Network News mailing

Ralph A. Shaw

Information protection in Europe

Steve Bellovin

Re: Losing systems -- and Structured Programming

Henry Spencer

Lynn R Grant

Steven C. Den Beste

Re: Ground proximity warning

**Henry Spencer** 

WORM storage and archival records

**RAMontante** 

Re: 3 vs. 2 engined airplanes

**Steve Jay** 

Re: Hackers break open US bank networks

Jan Wolitzky

Evidence

**Bill Murray** 

Info on RISKS (comp.risks)

Speak nicely to your air hostess - or be blacklisted...

<HCART%VAX.OXFORD.AC.UK@CUNYVM.CUNY.EDU> Mon, 16 JAN 89 17:47:27 GMT

From "Computing", January 12, 1989.

US airline TWA is under investigation by the Data Protection Registrar after a passenger saw abusive information on a computer screen, describing him as "obnoxious".

London-based systems engineer David Burns saw the screen when he

inquired about some lost luggage on returning to Los Angeles airport from Hawaii in October. He asked for a screen print and found it contained details of all the comments he had made to TWA staff including 'Pax (passenger) said do something constructive', 'Pax hung up phone', 'Pax obnoxious'. He said most of the details were not entirely accurate.

Burns wrote to the Data Protection Registrar after being given conflicting information by TWA about whether the records were deleted when the lost baggage was eventually found, or were kept for reference.

John Lamidey, the assistant data protection registrar in charge of investigations, said Burns' complaints are 'enough for me to think we should look at it further'. He appointed an investigator to visit TWA and expects to report back this month.

Burns said that, after returning from holiday and eventually recovering the lost suitcase from another airline, he rang TWA Baggage Services in London to see if the luggage was still recorded as missing. He was told it was.

Three people, including the head of passenger service, told him the report which contained his details could not be given to him as it was not company policy, even though the data was kept on the system for three months.

He then requested the information under the Data Protection Act.

[[which gives those in the UK the right to see information held on computers about them, with certain exceptions dictated by national security, etc.]]

Brian Johnson, manager of personnel and administration for TWA in the UK, wrote back to say 'no material is held by TWA by way of magnetic media which contains your name.' A TWA official said the data had been deleted.

## (Too) Intelligent Network News mailing

Ralph A. Shaw <ras@rayssd.RAY.COM> Fri, 13 Jan 89 12:55:07 est

Something I got in the mail today sounded more Orwellian than I liked, I thought I would pass it along. It was part of a subscription recruitment mailing from Intelligent Network News of Alexandria, Va. (Any security-minded Intelligence organizations based in Alexandria you can think of? :?)

>"Intelligent networks will dominate our industry's future and force every >company to rethink the way they do business.

>

>For example:

>

> Someday the public switched telephone network might track you >down in New York to tell you, "There's a leak in the basement of your >house in Denver. The plumber has already been called. He's reviewed >the service history of yoyur address, and thinks that it's probably >time to replace the blow-out valve on your water heater. Please respond." >The repair could be complete, further damage avoided, and the bill >paid by the time you return home, all thanks to nationwide intelligent >network services.

> .....

>Clearly, this evolution will create money-making opportunities for >those with the will and wits to recognize them.

Yes, just what I'm afraid of...

--

Ralph Shaw Raytheon Co. (SSD) <ras@rayssd.ray.com>

## Information protection in Europe

<smb@research.att.com>
Tue, 17 Jan 89 22:53:51 EST

The October '88 issue of Cryptologia has an interesting article entitled "European Needs and Attitudes Towards Information Security". The author (a founder of a firm that devises cryptographic algorithms, and hence not an unbiased source) claims that the free market is driving banks and other financial institutions towards better protection of their data; he asserts that banks have suffered a loss of business when their inability to keep data confidential has been demonstrated.

Of particular interest to this audience is his description of the (perceived) threats in Europe.

Europeans do not particularly need protection against "hackers" or petty criminals. They need protection against organized crime, major corporations and governments. Such opponents are characterized by the presence of serious motivation (and therefor the willingness to expend significant sums to attack a system), access to substantial resources, and the possession or ability to purchase whatever technological expertise is required.

He then goes on to relate three actual attacks. In the first, organized crime invested \$5,000,000 up front in technical preparations; the gain (actual or potential isn't clear from the article) is estimated to be 100 times that. The second involves a government spying on bank data in another country; he implies, though does not state, that it was the U.S. government that did the spying. Apparently, the bank suffered serious loss of business when its vulnerability became known. Finally, he describes the plight of "extractive industries", whose competitors, both private and state-owned, regularly mount sophisticated electronic spying operations against them.

If the claims are accurate, the difference in attitudes is fascinating.

--Steve Bellovin

# Re: Losing systems -- and Structured Programming

<attcan!utzoo!henry@uunet.UU.NET> Wed, 18 Jan 89 00:19:21 EST

It is worth remembering that the original meaning of "structured programming" followed the English usage in which "structured" means, approximately, "organized", and that the usage or non-usage of certain control constructs was suggested as a means to that end, not an end in itself. One can often get a good laugh by doing a global substitution of "organized" for "structured" in a pronunciamento from either side -- it tends to make both sides' arguments sound ridiculous. As it should: it is silly to confuse organization with a list of permitted constructs, and equally silly to criticize the desire for well-organized code on the basis of such confusion.

Henry Spencer at U of Toronto Zoology

#### Structured Programming

Lynn R Grant <Grant@DOCKMASTER.ARPA> Wed, 18 Jan 89 12:43 EST

I have been a proponent of structured programming for many years, and I have found that there is really only one rule: think about the poor guy who is going to have to maintain the program you are writing. All the other rules about indentation and goto-lessness simply follow from that.

The guy who ends up maintaining your program may be some rookie, or it may be a busy programmer who doesn't have time to carefully scrutinize your code, or it may be you six months down the road, after you've forgotten what you had in mind when you wrote the program.

Whatever you can do to make it easier for this guy to understand your program will cut down the chances for errors (and will keep him from putting you on his bad-guy list after having to fight with your code).

Lynn Gran
Technical Consultant
Computer Associates International, Inc.

#### re: Losing Systems

<denbeste@BBN.COM>
Wed, 18 Jan 89 10:12:51 -0500

In Risks 8.9, David Marks (djm408@tijc02.UUCP) lays much of the blame for

"losing systems" on the narrow attitude of management which they derived from the educational system.

Briefly, his reasoning goes:

- 1. Business types don't learn about computers and don't care about them
- 2. Engineers don't learn about business and don't care about it
- 3. There is therefore no common ground on which to meet.

Premise 2 is nearly completely true - the average software engineer couldn't care less about the realities of business. But I have not found Premise 1 to be true to anything like the same extent. No matter where I've worked, I am constantly running into business folks who are trying to understand computers - out of intellectual interest, "nift" factor, or the obvious fact that there is a shortage of computer-literate business people and thus it is a good way to advance a career (and the free market wins again...).

I think that there is an entirely different reason for the failure of the projects cited three or four references ago: Usually a project like this is specified not by the ultimate users of the service the computer will provide, but rather by a supplier in the form of a consultant contracted to buy the hardware and write the software. The consultant has no vested interest in the resulting software working correctly - he only has a vested interest in the project being big and expensive. The consultant wins once the contract is signed - everything after that is less important.

If those who have the need have no control, and those who have control have no need, then disaster will always strike. It doesn't even matter if they are talking to each other.

Steven C. Den Beste, BBN Communications Corp., Cambridge MA denbeste@bbn.com(ARPA/CSNET/UUCP) harvard!bbn.com!denbeste(UUCP)

## Re: Ground proximity warning

<attcan!utzoo!henry@uunet.UU.NET> Wed, 18 Jan 89 00:19:41 EST

- > "Note: the GPWS will not provide a warning if an airplane is flying
- > directly towards a vertical cliff."

It's worth noting that solutions to this have been proposed and rejected. The problem with the standard GPWS is that it basically looks down, not forward, so it fails in the presence of abruptly-changing terrain. (The vertical cliff is only the extreme case; rapidly-rising terrain will give a warning, but often too late for it to be useful.) At least one company has proposed a more sophisticated scheme in which the "warning surface", so to speak, is not a point underneath the aircraft but a sort of ski-shaped surface extending a considerable distance forward. Nobody was interested, so the proposal was shelved.

Henry Spencer at U of Toronto Zoology

#### WORM storage and archival records

RAMontante <bobmon@iuvax.cs.indiana.edu> Wed, 18 Jan 89 00:46:42 EST

Steve Phillipson proposes once-writable storage as a means to guarantee that archival records have not been tampered with. The idea is that the information, once recorded, can't be changed. The idea is fundamentally flawed, however, for reasons involving the digital nature of most such media.

Typed or handwritten documents, photographs, audio tape recordings, all could be trusted (once) because you could detect alterations in them, AND ALSO because you could determine that the item you had was the original. The letters on a ypewriter have "personalized" defects, for example. More to the point, tape recorders and cameras add their own high-frequency losses or image blurs to the signals they record; and if you make a copy of the original tape or photo, there is unavoidable degradation of the information and addition of machine-related "noise" to brand the copy as such. Analog video tape is another example -- broadcast quality tapes are unusable after a few generations of copying.

Digital media don't suffer from this degradation, though. I get a new program for my PC at home, put a blank disk of the same brand in the machine, and type "DISKCOPY". Strip the label off, and you can't tell which disk is the original. By the same token, if I have my "archived" Shakespearean sonnets on a WORM disk, I simply read an image of the disk into memory, edit a few lines and write the new image onto a fresh WORM disk. Presto -- bogus Shakespeare on a "tamper-proof" disk.

#### Re: 3 vs. 2 engined airplanes

Steve Jay <shj@ultra.UUCP> Tue, 17 Jan 89 21:38:36 PST

In RISKS 8.9, Jordan Brown says

- > I don't believe a 727 can fly on one engine. It must have two.
- > A three-engine airplane has a higher probability of having a failure in
- > the first place, and when it does have a failure it then has two points
- > of failure, EITHER of which will cause an accident.

I think he's wrong on both counts. I have no specific knowledge in this area, but I'm almost certain that a 727 CAN maintain level flight, at least a some altitudes, on one engine. Also, there was a highly publicized incident a couple of years ago when a Lockheed TriStar flying out of Florida almost crashed into the ocean because a mechanic had left out oil seals after maintenance on all three engines. As I remember it, the pilot got back safely only because he was able to keep one engine going.

Even if a 3 engine plane can't stay level on one engine, it will certainly

have a much lower rate of decent with one engine going than with none, giving the pilot a lot longer to deal with the problem or find a landing spot.

Even assuming that a 3 engined plane needs two engines to fly, the odds of 2 engines failing on a 3 engined plane are much, much, smaller than the odds of 1 engine failing on a 2 engined plane.

Steve Jay domain: shj@ultra.com

Ultra Network Technologies Internet: ultra!shj@ames.arc.nasa.gov

101 Daggett Drive uucp: ...ames!ultra!shj

San Jose, CA 95134 408-922-0100

## ★ Re: Hackers break open US bank networks

<wolit@research.att.com>
Wed, 18 Jan 89 09:13 EST

Australian authorities are working around the clock ... leaks of supposedly securedial-up numbers for US defence sites, including anti-ballistic missile launch silos, ...

The U.S. hasn't had any anti-ballistic missiles for more than a decade. I can only assume that the rest of the article is as accurate, especially since I've seen nothing about the "break-in" in the papers or news wires in this country.

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

#### Evidence

<WHMurray@DOCKMASTER.ARPA> Wed, 18 Jan 89 12:15 EST

In recent issues of RISKS, various people have lamented the loss
 of confidence we are experiencing in archival records kept by computer.
 The problem seems to me less of a computer problem than a media problem,
 specifically, choosing media that is appropriate for archival storage.

Would God that it were that simple. If freedom from modification were the only requirement for the medium, then there might be a solution. However, for an increasing number of applications light in glassor electricity in copper are the medium of choice for other reasons.

We require controls for the integrity and confidentiality of data that are independent of both media and environment, and which can move with the data.

Fortunately for us they are here. Digital signatures and envelopes can be combined to mimic the

behavior of the media and environmental controls that we commonly use. All that is required is a little bit of trusted storage in which to store the private keys and a tiny trusted process in which to do the code conversions.

Of course, I have just stated the requirement for both media and environmental controls. While they are still necessary, they are no longer sufficient.

William Hugh Murray, Ernst & Whinney



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 8: Issue 11

# Thursday 19 January 1989

## **Contents**

Risks of no backup systems for critical applications

Yoram Eisenstadter

Computer malfunction downs traffic lights, one killed, one injured Scott Campbell

Chaos Theory Predicts Unpredictability

China accused of software piracy

**PGN** 

Friday the 13th Again

**PGN** 

Computer error locks out politicians

D. Steele

Re: Losing Systems

Jerome H. Saltzer

Technical brilliance v. commercial acumen

Jerry Harper

National Credit Information Network

Sidney Marshall

Re: Ethics of the Internet

John Gilmore

RISKs of reading newspapers: Credit card fraud is not hacking.

Mike Van Pelt

Counting engines

**Don Alvarez** 

Info on RISKS (comp.risks)

## Risks of not having backup systems for critical applications

Yoram Eisenstadter <yoram@garfield.cs.columbia.edu> Thu, 19 Jan 89 00:16:37 EST

The following article, which appeared in the "Metropolitan Diary" section of today's New York Times, illustrates the risk of not having backup systems for super-critical computerized applications.

The other day, Gloria Ross was late for an appointment at a company on the Avenue of the Americas. She holds herself blameless for being tardy and in defense she offers this explanation:

The high-technology building where the company has its offices has a computerized directory. To find the floor of the person you wish to visit, you push a button with the first letter of the last name.

Aware of this procedure, Ms. Ross pressed the button marked "O" on one of the computer monitors mounted on a large black column. Nothing happened. A guard told her to try the next column. Again, nothing. The computer was down. Her next stop: the information desk in the lobby.

"I get my information the same way you do, lady," the man at the desk said, informing her that even he did not have a printed directory...

The article goes on to describe the chaos that ensued in the building, with "dozens of people desperately cruising from floor to floor" looking for the right offices. Let's hope that the building's managers learned the obvious lesson from this incident.

## ✓ Computer malfunction downs traffic lights. One killed, one injured.

Peter Neumann <neumann@csl.sri.com> Wed, 18 Jan 1989 22:48:49 PST

One child was killed and another injured [Mon 9 Jan 1989] when they were hit by a truck after entering a crosswalk where the pedestrian signals were not working. The malfunction was caused by a computer error that affected traffic signals at 22 school crossings. The pedestrian signal cycles failed to switch to the school schedule. The cause reportedly may have been a breakdown in the radio communications between a computer in Colorado Springs and an atomic clock in Boulder. [Colo Spgs Gazette Telegraph, 10 and 11 Jan 1989; contributed by Scott Campbell, PAR Gov't Sys Corp, Colo Spgs.]

## Chaos Theory Predicts Unpredictability

Peter Neumann <neumann@csl.sri.com> Wed, 18 Jan 1989 22:39:33 PST

A physicist who applied the new mathematics of `chaos theory' to the Star Wars missile shield foudn that the equations pointed again and again to crisis and war or -- at best -- a continued and precarious balance of terror. ``The question is not really Star Wars, but what do you do if all you can predict is unpredictableness?'' Alvin M. Saperstein of Wayne State University asked [at the AAAS meeting in San Francisco]. [From an article by Charles Petit, SF Chronicle, 18 Jan 1989, p. A18]

#### China accused of software piracy

Peter Neumann <neumann@csl.sri.com> Wed, 18 Jan 1989 22:32:31 PST

Beijing (Washington Post, 18 Jan 1989) -American companies are losing "many millions" of dollars in potential business in China because the companies' computer softwae has been widely pirated... China has no copyright law of its own...

#### Friday the 13th Again

Peter Neumann <neumann@csl.sri.com> Wed, 18 Jan 1989 22:28:34 PST

There were various reports of Friday-the-13th virus deletions in Britain, attacking MS-DOS systems. The so-called virus "has been frisky and hundreds of people, including a large firm with over 400 computers, have telephoned with their problems," according to Alan Solomon, director of S and S Enterprises, a data recovery center in Chesham. The virus reportedly bore similarities to the Friday the 13th Israeli virus (13 May 1988, the previous Friday the 13th). [Source: SF Chronicle, 14 Jan 1989, p. B1]

#### Computer error locks out politicians

D. Steele <uivkey@NADC.ARPA> Thu, 19 Jan 89 09:27:15 EST

Just to show that computer systems play no favorites in politics, local news reports are blaming a computer error for denying Pennsylvania Republicans tickets and access to many of the Presidential inauguration balls and festivities. The politicians are complaning "its like being all dressed up with no place to go".

Submitted by Scott Berger, Naval Air Development Center, Warminster, PA

#### re: Losing Systems

Jerome H. Saltzer <Saltzer@LCS.MIT.Edu> Thu, 19 Jan 89 12:31:05 gmt

The question as to why there are so many losing systems may have a simpler, more fundamental answer than has been suggested in the contributions over the last couple of weeks. So far, those contributions have (1) suggested incompetence in management or technical ability, and (2) questioned some of the currently fashionable magic bullets, such as structured programming.

I believe that the more fundamental answer is that the pace of improvement of hardware technology in the computer business has, for 35 years now, simply been

running faster than our ability to develop the necessary experience to use it effectively, safely, and without big mistakes.

The losing systems almost always contain some elements of newness; in fact on close inspection they usually contain several such elements. (If someone claims there is nothing new in a project that involves software development, then ask why they aren't just using previously existing software. It is the attraction of taking advantage of new possibilities, usually as the result of hardware being either more functional or cheaper than it used to be, that leads to new software systems.) If these new elements were to arrive on the scene one at a time, and spaced far enough apart that thorough experience could be assimilated with each previous new element, then I submit that traditional engineering practice, as applied to pyramids, cathedrals, bridges, consumer electronics, and even airplanes, would lead to higher success probabilities. Mistakes would still be made, but they would tend to occur on the far-out projects that are expected to carry an element of risk, rather than the ones that intuitively seem like they ought to be routine, such as automating the county records.

Arguing that managers should become computer wizards, or offering structured programming to fix the problem, just don't seem to me to get to the heart of this more fundamental issue.

When the technology ground rules change at a rate that is ten times faster than in other engineering disciplines, it would seem that unless one can figure out how to accumulate and assimilate experience also at a ten-times-faster rate, system failures are an expected result. Perhaps a more interesting question is how it is that some computer systems manage to be successful. I observe two related things that are often associated with successful systems:

- 1. Those systems that are successful are usually conservative, with somewhat simpler objectives than the state of technology would have permitted.
- 2. Systems that are successful often had the management advantage of a system dictator who had the absolute power to say NO to ideas that didn't seem to fit in. A dictator is one of the few mechanisms that can keep an implementation conservative in the face of pressures to be state-of-the-art.

My conclusion from these observations is that since: (1) it is hard to be conservative in the face of tempting technology advances; and (2) appointing dictators isn't a common management practice; successful systems aren't very common either. And having conservative goals and a dictator doesn't guarantee that the system will be winning or that its future users will like it, it just sets the stage for that possibility.

Jerry Saltzer

#### Technical brilliance v. commercial acumen

Jerry Harper <jharper@euroies.UUCP> Thu, 19 Jan 89 15:34:31 GMT Steven C. Beste made the point that managers are trying to come to grips with computer technology moreso now than ever before; this I would generally agree with subject to the caveat that the degree of managerial immersement in the technology will never match that of the technical expert. One of the last companies I was consultant to actually lost sales because the management didn't understand either the product or the market, and knowing both was especially important as the company was making the transition from conventional DP through Cobol to providing a logic programming environment on a mainframe. The permanent technical staff couldn't have sold their souls for ice pops and the management were having fiercesome difficulty in making the paradigmatic shift from Cobol inspired projects to AI (expert system bespoke applications). Just as you thought the management was grasping the core issues Sisyphus would pop up and roll progress back. Even more lamentable were the salesforce who new sweet f.a. about either methodology. Because AI was "sexy" the salespeople were inclined to promise the earth (one salesman reckoned he had a contract for a complete CASE system for a major motor manufacturer in the UK even though neither he nor the company had any experience in this area) and take umbrage when it was explained that the company simply couldn't deliver. The net result was that the company became unsatisfactory for quite a number of the technical people who carried their skills elsewhere. Nevertheless, observing the company's progress from a distance it seems to be doing quite well and the mangement have made the learning curve.

#### National Credit Information Network

<marshall.wbst@Xerox.COM> 18 Jan 89 15:50 EST

I just received in the mail as part of the BYTE magazine package of postcards from manufacturers etc. a post card selling a program capable of accessing the National Credit Information Network (if I qualify). Here is the text of the postcard (the typography of the card was ragged and this is as exact as I could make it):

NATIONAL CREDIT INFORMATION NETWORK
ON-LINE ACCESS PACKAGE

AVOID SLOW PAY - NO PAY HIRE QUALITY EMPLOYEES

SAVE \$200.00 \$498.00 \* SAVE \$200.00



IF YOU QUALIFY FOR ACCESS...THIS INFORMATION IS IDEAL FOR:



FREE ON-LINE DEMO

"MONEY-BACK GUARANTEE
IF YOU DO NOT QUALIFY



After connection, slowly press the [ENTER] key 4 times. When prompted for a Username: type DECK4 then press [ENTER]



Is this scary or what?

--Sidney Marshall



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 8: Issue 12

# Friday 20 January 1989

## **Contents**

Risk of using your own name

Gary T

- Risks in NBS time by radio (computer malfunction downs lights) Clements
- Computer-related accidents in British chemical industry Jon Jacky

Re: Losing Systems

**Henry Spencer** 

**Donald Lindsay** 

**Keane Arase** 

- Failure of Software Projects
  - **WHMurray**
- Re: Structured Programming

David Collier-Brown

Jerry Schwarz

Discrete probability and airplanes

Mike Olson

Re: Chaos theory

Phil Goetz

Info on RISKS (comp.risks)

## Risk of using your own name

<garyt@cup.portal.com> Fri, 20-Jan-89 09:37:56 PST

Computergram Number 1098 (published by Apt Data Services in London) featured a story from Newsbytes that illustrates the risk of using your own name to test a computer program. Michelle Gordon, training as a police dispatcher in Bloomfield, Connecticut, was told by her instructor to use her own name as a test case to see how the computer reports outstanding "wants and warrants" against an individual. Michelle did so -- and was shocked to find out that she was wanted for passing a bad check! Back in July, she had written a \$90.97 check to a clothing store, and the check had bounced. After turning herself

in, she was relieved of duty -- but the police say that she should get her job back once the bill has been paid.

[I notice Gary did not use HIS name. PGN]

#### Risks in NBS time by radio: Computer malfunction downs traffic lights.

<clements@DIP.BBN.COM>
Fri, 20 Jan 89 13:11:09 -0500

- > ... The cause reportedly may have been a breakdown in the radio
- > communications between a computer in Colorado Springs and an atomic
- > clock in Boulder. ... (Re: RISKS-8.11)

I'll guess that this radio communications system is the NBS transmissions from WWV in Fort Collins (which is synchronized to Boulder).

Aside from the obvious risks in designing a system the way this one (the traffic signals) was apparently done, the transmission code used by WWV is inherently risky. There is no parity check on the data in the code. (And only day of year, not year, which is another story with its own risks.)

Receiving clocks must compare successive samples of the code, which is BCD-ish and has a one minute cycle, and see whether the samples are in the correct sequence. Eventually the clock decides it has correctly read the code. But if a static burst or radio fade garbles the same bit in the code for a few minutes the clock will set to the wrong time. The Heath "Most Accurate Clock" reads these transmissions and fails in this way. A couple of times a year I will see my clock confidently displaying a time which is EXACTLY 4 hours wrong or EXACTLY 20 minutes wrong.

#### Computer-related accidents in British chemical industry

<JON.JACKY@GAFFER.RAD.WASHINGTON.EDU>
20 Jan 1989 11:27:53 EST

Here are some interesting examples of hardware-software-user interaction from the British trade magazine, CONTROL AND INSTRUMENTATION, Vol 20 No 10, October 1988, pps. 57, 59:

Wise After the Event by Trevor Kletz

... Computer hardware faults do occur. ... Their effects can be reduced by installing `watch-dogs.' However, an error in a watch-dog card actually caused one accident --- valves were opened at the wrong time and several tons of hot liquid were spilt [ref 1].

...In one plant, a pump and various pipelines were used for several different duties -- for transferring methanol from a road tanker to storage, for charging it to the plant and for moving recovered methanol back from the plant. A computer set the various valves, monitored their positions and switched the transfer pump on and off. On the occasion in question, a road tanker

was emptied. The pump had been started from the panel, but had been stopped by means of a local button. The next job was to transfer some methanol from storage to the plant. The computer set the valves, but as the pump had been stopped manually it had to be started manually. When the transfer was complete the PES [Programmable Electronic System --- British for computer control system - JJ] told the pump to stop, but as it had been started manually it did not stop and a spillage occured [ref 5].

... Another incident occured on a pressure filter which was controlled by a PES. It circulated a liquor through a filter ... As more solid was deposited on the filter the pressure drop increased. To measure the pressure drop, the computer counted up the number of times that tyhe pressure of the air in the filter needed to be topped up in 15 minutes. It had been told that if less than five top-ups were needed, filtration was complete ... If more than five top-ups were needed, the liquor was circulated for a further two hours. Unfortunately a leak of compressed air into the filter occured which misled the computer into thinking that the filtration was complete. It signalled this fiction to the operator who opened the filter door --- and the entire batch, liquid and solid, was spilt. ... The system had detected that something was wrong, but the operator either ignored this warning sign or did not appreciate its significance [ref 2].

... (In one incident) when a power failure occured on one site the computer printed a long list of alarms. The operator did not know what had caused the upset and did nothing. After a few minutes an explosion occured. Afterwards the designer admitted that he had overloaded the operator with too much information, but he asked why the individual had not assumed the worst and tripped the plant?

... (In another incident) a computer was taken off-line so that the program could be changed. At the time it was counting the revolutions on a metering pump which was feeding a batch reactor. When the computer was put back on line it continued counting where it had left off --- with the result that the reactor was overcharged.

References (included in the article)

- 1. I Nimmo, SR Nunns, and BW Eddershaw, Lessons learned from the failure of a computer system controlling a nylon polymer plant. Safety and Reliability Society Symposium, Altrincham, UK, Nov 1987.
- 2. Chemical Safety Summary, Vol 56, No 221, 1985, p. 6, (Published by Chemical Industries Association, London).
- Jonathan Jacky, University of Washington

#### Re: Losing Systems

<attcan!utzoo!henry@uunet.UU.NET> Fri, 20 Jan 89 00:21:32 EST

>Managers see knowledge about computing only useful to engineers and

>programmers. Business schools for the most part do not teach computer >literacy, nor how a non-technical manager should deal with a large software >system in his company...

This is actually part of a larger problem. I recall reading an interview with a Japanese business-methods type lecturing in the US. One of the first things he asks his students to do is solve a simple quadratic equation. Many of them are baffled; most are offended. He then explains to them, as gently as possible, that one cannot do any form of optimization (of costs, production rate, whatever) without solving quadratics (at least). North American business schools, by and large, have the same preoccupations as North American businesses: mergers, acquisitions, advertising, and legal maneuvering, as opposed to making better products at lower cost. The problem, increasingly, is not that managers are ignorant of technical issues, but that they consider them unimportant. The ignorance is an effect, not a cause.

Henry Spencer at U of Toronto Zoology

## Re: Losing Systems

<Donald.Lindsay@K.GP.CS.CMU.EDU>
Fri, 20 Jan 1989 13:21-EDT

>From: Jerome H. Saltzer <Saltzer@LCS.MIT.Edu>
>I believe that the more fundamental answer is that the pace of
>improvement of hardware technology in the computer business has, for 35
>years now, simply been running faster than our ability to develop the
>necessary experience to use it effectively, safely, and without big
>mistakes.

I don't think it's "developing" experience: it's spreading experience.

The technology has given us:

- 1. online systems (terminals), which led to:
  - distributed systems
  - interactive human interfaces
- 2. speed, price, reliability, and all that.

I don't think that the failures stem from our progress on Point 1. We had online systems in the 1960's. Those development projects were seen as big, expensive, hairy projects that entailed risk. Now that similar projects are cheap, the difficulty is somehow overlooked. Take, for example, the municipal system that started this debate. It was unusable because it did not integrate well into the complex environment that the projected users were already coping with. We had failures like that in the 1960's. I would blame our advanced technology, not for raising deep issues, but for putting big problems into a multitude of small hands.

Don lindsay@k.gp.cs.cmu.edu CMU Computer Science

## Re: Losing Systems

"Keane Arase" <kean%tank@oddjob.uchicago.edu> Fri, 20 Jan 89 09:09:07 CST

I can add some first hand information about losing systems. Let me tell you a story about a data collection manufacturing pacakge I stayed as far away as possible from.

Background: This was a marketing intensive company. This company considers technical support people expendable. They would rather lose their experienced people because programmers/analysts coming out of school are cheaper. BTW, they hired on grade point average only. Not what you know, but what you did in school. In my experience, the two are \*not\* the same.

It was decided we were to develop an off-the-shelf/base package which could be custom modifiable for data collection/time and attendance functions for the manufacturing environment. Because of a recent reorganization, all of the experienced project leaders and programmers \*fled\* the company.

Our most experienced project leader (hat was left) had stated he was leaving in 6 weeks because of personal reasons. Yet the project planning and design was given to him to do. Six weeks later, he left, the project design about 30% completed. Another person (from another area in the country) was brought in to complete the design. Soon after the design was completed, \*he\* left the company because of a better offer elsewhere. Thus, we had no one who completely knew the entire system design. Worse, none of the programmers knew the manufacturing environment, so they couldn't spot any design errors, even if they stared them in the face.

Since the reorganization made us a profit center, we now \*had\* to make money. This, of course, while 90% of our efforts went toward development of a product which was projected to make money in \*two\* years. Because we were in the red, raises were denied to certain programmers (through no fault of their own), who in turn did extremely shoddy work in the programs they put together. (And of course, left at first opportunity.) Our regional manager also declared that we would receive no new hardware, since we couldn't justify the cost because we were losing money. Thus, we didn't have the necessary hardware that this package was supposed to be running on. (Only later did marketing force our regional manager to get the equipment. Much of the equipment belonged to our certification, verification and testing site.)

Because the project was losing money and behind schedule, programmers were \*required\* to work 45 hours per week. No compensation, no exception. Several more programmers \*fled\* the company. They hired part time people to fill in the losses. (Sorry, can't hire more people. Can't justify the cost!)

In the scheduling, there was no provision for extensive system testing, or for the development of test scripts. More delays, more time and money lost.

Because we were losing money, the company decided our district was expendable and desolved our group. We were given the option to move to a medium sized city in Southern Ohio, where their home headquarters is. \*No one went\*. Thus, this company had a \$300K+ package, somewhat complete (about 250K to 350K lines), but far from working correctly, with NO ONE ON THE ORGINAL OR SUBSEQUENT PROJECT TEAMS LEFT IN THE COMPANY! (From the spies I have in the

company, they hired a bunch of college kids straight out of school to complete the work under 2 experienced project leaders.)

This post details about 40% of the problems encountered during the development. It doesn't include poor hardware design, or the fact this package is really to extensive to run on the recommended hardware. Even with all that went wrong, this company is still marketing this package today, training people how to sell it and install it. (The base package is more or less useless without modification.) I'll bet it still doesn't work today.

I think I can summarized why projects fail by the following:

Poor planning and quality control. By far the worst offender. How can you keep within budget and time frame if certain critical events are left out of the schedule?

Poor management and company policy. This is probably the second worst offender, although I'd probably tie it for number one. Management is only interested in one thing. The bottom line. Does it make money NOW? (Apologies to those managers who aren't this way. But I'll bet if you work for a large computer corporation, and your year end bonus depends on how much your site makes, you \*are\* one of these.) They must also provide the necessary resources to get the project done. This includes keeping your people and treating them right. (At least until everything works! :-) Also, managers who know nothing about the computer biz or the programming environment, should be managing the sanitation engineers or the cafeteria staff. They have no business managing things they know nothing about.

Poor expertise by programmers. This is not necessarily the programmers fault, but the companies fault for not providing the education. (Please note this assumes competent people! If the human resources department does their work properly, getting competent people shouldn't be a \*big\* problem.) Programmers should know what they're programming \*for\* as well as what the programs should do. Programmers should also know the project. I had enough pull and technical expertise to be involved in \*other\* failing projects. (Want to hear others? E-mail me, and if I have the time I'll detail others.)

Keane Arase, Systems Programmer, University of Chicago Disclaimer: This company was \*not\* the University of Chicago!

#### Failure of Software Projects

Jerry Saltzer suggests that the trouble with software is the speed of advance in hardware; that the software developer is overwhelmed by the new function and opportunity. Else, he suggests, normal engineering discipline would suffice.

I would like to suggest that it would suffice anyway if it were applied. The difficulty is that software is managed by programmers, not engineers. Programmers have no tradition of quality of their own and insist that their

activity is so different from what engineers do, that engineers have nothing to teach them.

Suppose that you had been an electronics engineer in 1960 but had been out of the field since. Don't you think that you would see more product complexity and risk if you re-entered today? Engineering discipline has been adequate to cope there. It would be able to cope in software too, if only it were regularly applied.

I am hopeful that the use of the term "case" presages the application of more discipline in programming.

I also draw hope from the entreprenurial development of software for the market, as opposed to works built for hire for a single organization. I saw a great deal of quality software at Egghead on Saturday.

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: Structured Programming

David Collier-Brown <dave@lethe.UUCP> 20 Jan 89 02:21:37 GMT

horning@src.dec.com (Jim Horning) comments:

- > I read Bruce Karsh's diatribe with incredulity. He conjures up from thin
- > air a straw man to denounce. I simply cannot find any contact between the
- > "structured programming" that he talks about and structured programming as
- > it is understood in the computer science and software engineering communities.

Fair enough, but he is describing an understanding which is very prevalent in the industry... Many managers from the pre-structured era understand structured programming to be just what was described: a supposed panacea.

The academic community does not even know the difference. In faculty "A" of our major local university, it is understood as a suite of complexity-management tools, mostly the "mental tool" sort. In faculty "B" it is understood, if at all, as a rule-set which is supposed to produce correct programs.

Any of my last three major employers contained people who took opposing views on the meaning of structured programming. What I found significant was that the people who regarded it as a tool also knew its weaknesses and knew other tools and techniques.. The people who claimed it was a panacea invariably knew no other technique for improving program quality.

It sounds like Bruce worked for one of the snake-oil salesmen and did not have the opportunity to see it used by a professional or academic software engineer. And yes, I agree with him that using it as snake oil has placed us at risk.

--dave (when faced with strawman, pull stuffing out) c-b

## Structured Programming

Jerry Schwarz Wed, 18 Jan 89 20:25:34 EST

Arguments about the influence of structured programming seem slightly old fashioned to me. In the circles I travel in "object oriented" is the hot new buzzword.

Jerry Schwarz

### Discrete probability and airplanes

Mike Olson <mao@blia.UUCP> 19 Jan 89 12:34:40 PST (Thu)

In RISKS 8.10, steve jay (shj@ultra.com) comments

- > Even assuming that a 3 engined plane needs two engines to fly,
- > the odds of 2 engines failing on a 3 engined plane are much, much,
- > smaller than the odds of 1 engine failing on a 2 engined plane.

this is essentially true, with the ordinary mind-bending caveats that probability theory imposes. if the probability of a single engine failing is p, then the probability of one of three engines failing is 3p (this is actually the expected value of the random variable that maps failure to one, and non-failure to zero, but it'll serve). p is a real number between zero and one, by the way. in this case, we can assume that it's closer to zero than to one.

the probability of two of three engines failing is 6(p\*\*2), since the probability of one engine failing is 3p, and the probability of one of the remaining two failing is 2p, and we multiply (since they're independent events -- the proof is sort of hairy for our purposes).

all this is true, of course, as long as all the engines are working. as soon as one fails, the overall probability of failure changes. for example, the probability of two of three engines failing is  $6(p^{**}2)$ , as above. as we're flying along, one engine fails. oops. the probability that another engine will fail is 2p, and not the  $6(p^{**}2)$  that seems intuitively correct. airplane engines, like coins, have no memory -- or if they do, it's the wrong kind.

the risks? statements like "the odds of ... [failure] ... are much, much smaller" can be misleading. the debate here over the likelihood of failure is evidence of that -- a group of intelligent, educated people can't agree on the odds. numbers are tricky in this field, and don't always behave the way you'd expect them to.

when i was studying this stuff, a friend said to me, "the first thing to do

when a probability theorist asks you a question is to grab him by the throat, slam him up against the wall, and ask him, 'what do you MEAN?!?'" this is good advice. it's also a good idea to quantify things explicitly -- how \*much\* less likely is failure, when you add another engine? -- rather than to offer imprecise reassurance.

mike olson, britton lee, inc.

## Re: Chaos theory

<PGOETZ@LOYVAX.BITNET> Fri, 20 Jan 89 11:12 EST

I'd like to know just how applying chaos theory to a defense system shows ANY results at all about the stability of the political systems related to that system. The idea that you can mathematically prove the effects of one isolated system on the relations between two nations is absurd. The current thawing between the US and the USSR depends largely on the fact that Reagan and Gorbachev like each other. Could anybody have proved that 8 years ago? No.

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 8: Issue 13

Sunday 22 January 1989

## **Contents**

Gigabit superhighway/worms

Vint Cerf

IAB Ethics DRAFT

Vint Cerf

Space shuttle computer problems, 1981--1985

Jon Jacky

F-16 that can't stall falls from sky

Scot E Wilcoxon

Re: China accused of software piracy

Jim Olsen

Losing systems

**Dale Worley** 

**Chris Lewis** 

Re: Structured Programming

John Mainwaring

Mark Rosenstein

Steve Pozgaj

Info on RISKS (comp.risks)

## ✓ Gigabit superhighway/worms (RISKS-8.9)

<CERF@A.ISI.EDU> 23 Jan 1989 00:09-EST

In RISKS-8.9, Brad Blumenthal asks whether our legislators and their staff are aware of the similarity between the internet and the proposed multi-gigabit superhighway. I can assure Mr. Blumenthal that the question has arisen and has been posed to several members of the research community by members of the Congress responsible for scientific and technical matters. The worm affair made a strong impact on policy makers.

Vint Cerf

## IAB Ethics DRAFT (RISKS-8.8)

<CERF@A.ISI.EDU> 23 Jan 1989 00:09-EST

The copy of the IAB statement on ETHICS was a DRAFT copy circulated for internal comment by the IAB before final editing and release. I would be very interested to know how a copy happened to fall into Mr. Stoll's hands. Readers should be advised that the copy they saw is still subject to change until ratified by the IAB.

Vint Cerf

[By the way, subsequent to the appearance of RISKS-8.8, Cliff noted to me that he had accidentally omitted the author's name from the DRAFT. PGN]

## ✓ Space shuttle computer problems, 1981--1985

<jon@june.cs.washington.edu>
20 Jan 1989 15:27:13 EST

Here are excerpts from an article that appeared a week before the flight of the space shuttle Discovery last September:

NASA's close calls: lessons learned? by Richard Doherty, ELECTRONICS ENGINEERING TIMES, September 6, 1988, pps. 4,8.

... The House Science and Technology committee convened its own investigation of the (January 1986 Challenger accident) just days after the Rogers commission concluded its four-month effort. (Its findings are reported in) 'Investigation of the Challenger Accident, House Report 99-1016'. That report indicates ... dozens of failures in the shuttle's General Purpose Computer (GPC) and Avionics systems. ... NASA has reviewed these flight anomalies and decided that they fit within the acceptable risk criteria. Thus, it has not made any significant changes to system hardware or software for Discovery's launch. ... Most engineers tracking the shuttle program can recall very few reported avionics and computer-system failures during the program's 24 completed missions. Nevertheless, more than 700 anomalies involving computers and avionics have been logged by NASA. ...

[Here follow just a few of many examples from the EE TIMES article. Most seem to involve hardware or sensor failures. Several examples in the article are not computer- or even avionics-related. ]

STS-6, April 4, 1983: ... Landing gear must be manually deployed after computer fails to trigger its descent.

STS-9, November 28, 1983: Four hours before re-entry, pilot orients orbiter using RCS (Reaction Control System) steering jets. After jets fire, one computer crashes. A few minutes later, a second goes down [ There are four redundant GPC computers running identical software plus a fifth GPC running different backup software - JJ]. Pilot John Young delays landing while craft drifts in space. Then one of three Inertial Measurement Units fails. (Young

testified three years later: `Had we then activated the Backup Flight Software, loss of vehicle and crew would have resulted.' He now says problems have been resolved. Post-flight analysis shows each GPC failed when RCS jet motion jarred a piece of solder, shorting CPU boards).

Before landing, the second of three APU's (Auxilliary Power Units) fails. Fire and explosion occurs while orbiter is parked at its landing site. ... NASA engineers label this incident a `double-failure scenario that just beat all the probability odds.' ...

STS-19 (51-F) July 29, 1985: Three minutes into ascent, a failure in one of two thermocouples directs computer shutdown of center engine. Two minutes later, engine chamber pressure is indicated as zero. Mission control decides to Abort to Orbit. ... Challenger is in orbit 70 miles up, 50 miles lower than planned. Had shutdown occured a half-minute earlier, mission would have had to abort over the Atlantic. (NASA has reset some of the binary thermocouple limits via software changes).

STS-13 (41-G), November 5, 1984: ... Landing gear must be manually deployed after computer fails to trigger its descent.

- Jonathan Jacky, University of Washington

## **F-16** that can't stall falls from sky

Scot E Wilcoxon <sewilco@datapg.MN.ORG> Fri, 20 Jan 89 17:07:16 CST

Reprinted with permission from the Tampa Tribune, 23 December 1988, Page 1B

Crash of F-16 still unexplained by MacDill staff By STEVE HUETTEL, Tribune Staff Writer

TAMPA - Moments after an instructor warned 1st Lt. David S. Johnson that he might be flying too slowly, the student pilot's F-16 fighter stalled and plummeted into the Gulf of Mexico. Johnson ejected safely Sept. 9 and was back in the cockpit within a month. A month before he is due to graduate, MacDill Air Force Base officials still won't say whether the 24-year-old pilot was negligent or if an onboard computer designed to keep the \$9.5 million jet from stalling failed. But, crashing an F-16 isn't necessarily grounds for dismissal from the six-month course, they say.

"It's an environment where they're still learning the airplane, and mistakes can happen," said Capt. Dian Lawhon, a MacDill spokeswoman. "At that point, they might not have acquired some of the skills they need." Students can be yanked at any time, she said, for "gross pilot error."

Word that Johnson's jet stalled surprised the F-16's manufacturer and former pilots familiar with the fighter.

A computer inside the fighter should override any commands that would cause a stall, said Joe Thornton, a spokesman for General Dynamics in Fort Worth, Texas. "If a pilot tells the airplane to do anything the airplane doesn't want to do, the computer will take control of the airplane from the pilot," he said. "The pilots I talked to said you can't (stall) it."

But the computer is programmed only for common, dangerous flight configurations, said 1st Lt. Susan Brown, a MacDill spokeswoman. "It's not set up for every possible way you can get yourself into trouble," she said. Johnson, of Parker, Colo., did not return telephone calls to comment on the accident.

On the morning of Sept. 9, he was practicing fighter maneuvers with an instructor in a second plane over the Gulf west of Fort Myers. It was Johnson's seventh solo flight in the F-16. He had flown more than 200 missions in trainer aircraft, earning outstanding evaluations from his teachers at basic flight and fighter preparation schools.

Four times, the pilots flew a downward corkscrew maneuver in which Johnson tried to get behind the other aircraft to line up a gun or missile shot. Something went wrong as they broke off the exercise the last time. The Air Force won't release an investigation board's findings or statements by the pilots. But a heavily censored version of the report obtained under the federal Freedom of Information Act states that Johnson's F-16 stalled after he finished the last maneuver.

A drawing of the maneuver doesn't show Johnson's speed or altitude. The instructor pilot he trailed started at more than 400 mph but slowed to 150 mph as he climbed to 14,700 feet at the end of the exercise. "We got a little slow there, check your air speed," the instructor warned in a transcript of his radio conversation with Johnson. The student acknowledged the message, then disappeared from the instructor's sight.

The F-16 can stall at speeds of 230 mph or slower, depending on its weight and angle of flight, MacDill officials said. They declined to say what speed Johnson was flying when his plane stalled or the altitude at which he ejected. The report drawing depicts Johnson's jet in a near-vertical climb just before it stalled. "That should never have happened," said Howard Acosta, a former Navy pilot and St. Petersburg attorney who successfully sued General Dynamics on behalf of an F-16 pilot's widow last year. "The computer should change the angle of attack and get the wing flying again."

Unlike older aircraft, the F-16 has a fly-by-wire system that controls the flaps and engines through electrical impulses. The pilot's commands go through a computer that prevents the aircraft from getting into situations where it could stall or break apart from excessive gravity forces, say pilots. "It's designed not to stall," said a former F-16 pilot. "It's made to recover. You can take your hands off, and it'll fly."

Scot E. Wilcoxon sewilco@DataPg.MN.ORG {amdahl|hpda}!bungia!datapg!sewilco Data Progress UNIX masts & rigging +1 612-825-2607 uunet!datapg!sewilco

## Re: China accused of software piracy

Jim Olsen <olsen@XN.LL.MIT.EDU> Sun, 22 Jan 89 13:50:51 EDT

>American companies are losing "many millions" of dollars in potential >business in China because the companies' computer software has been >widely pirated... China has no copyright law of its own...

This is an example of the risk in assuming that the laws of one's own country apply (or ought to apply) everywhere. Copyright and patent protection are,

fundamentally, matters of internal law for each country. Foreign copyrights exist only via international copyright convention.

In a nation which is not signatory to a copyright convention, foreign copyright is invalid. However, authors in such a nation receive no international copyright protection. Each nation decides if such a tradeoff is in its best interests.

Thus, copying American computer programs in China is perfectly legal, and therefore does not deserve the term 'piracy'. American law does not apply in China, even if some American companies would like it to.

## Losing systems

Dale Worley <worley@compass.UUCP> Fri, 20 Jan 89 11:27:40 EST

Jerome Saltzer remarks that the domains of application of computers have been enlarging at an enormous rate. The rate at which computers become cheaper relative to number of them sold (the "experience curve") is no different from any other product. What is different about computers is the extraordinary price-sensitivity of potentially computerizable applications - a tiny drop in the price of computers introduces whole new application domains. This puts the computer industry into a rapid positive feedback loop of dropping prices, widening applications, and increasing unit sales.

I also agree with his remarks on how to manage computer-based projects, but you must remember that one result of these policies is that one will get somewhat less bang for the buck than the state of the art would tempt one to expect.

As far as managers are concerned, I'm reminded of a comment by Lester Thorow, dean of the MIT School of Management, regarding their new "managing technology" degree program: Many managers want to learn how to manage technology, but few want to learn about technology.

Certainly, American managers have little technical training, and few (especially in the upper echelons) want to acquire any. This has been blamed for the inability of American companies to deal with rapidly changing technology. In contrast, German and Japanese managers often have technical training and are reputed to be better at dealing with changing technology. Do they have a lower rate of computer project failure?

Dale Worley, Compass, Inc. compass!worley@think.com

#### ★ Re: Losing systems....

Chris Lewis <clewis%ecicrl%gate%tmsoft@csri.toronto.edu> 20 Jan 89 20:12:09 EST (Fri)

In <u>Risks 8.6</u>, Vince Manis postulates a number of hypothesis over how "megabuck systems ... go into the trashcan" after seeing reports of two such in <u>Risks 8.4</u>.

I can add another reason with an example (actually a "near failure"):

A Government creates the system by executive edict, without any technical study. Especially those in non-technical areas where the problem isn't well understood.

Which I expect is the actual reason for the failure of the first example in <u>risks 8.4</u>.

The second example in <u>Risks 8.4</u> is probably simply that there was \*no\* design control. In projects where there are multiple "customers", it is extremely important to have firm control vested in \*one\* person or small group of people. If you have dozens of people yammering for this feature or that, and nobody can or will say "no" to some of them, you're in \*deep\* trouble. The report on this system implied that this was one of the main reasons for failure.

Which is also why some language standards are so big....

#### My example:

The current incarnation of the Ontario Health Insurance Plan (Government run health insurance system, OHIP for short) was created by Government legislation (Ontario Health Insurance Act, 1972 - I think), to be in operation approximately 6 months later. At the time, the Ministry of Health didn't have much of a DP dept., nor had there been \*any\* technical study.

When I studied this system for a Royal Commission back in '79, I can't help remembering how awestruck I was that they actually had the monster in operation at 6 months. Startup from zero staff, resource or facilities. Awesome. They then paid for it with two or three years of continuous firefighting. The only reason that they succeeded was that they had lucked into some of the best DP people/managers I've \*ever\* met.

As well as some of the worst senior administrative people I've ever had the misfortune to meet.

This application is still probably the biggest single DP application in the entire province - 13 master files (one of which was 70 reels of 6250 BPI tape back in '79), oh about 12 main programs and had to be run on a 48 hour cycle. It took somewhere near 24 hours to run on their machine as of '77: 370/168 I believe.

The head analyst gave me a report discussing a lot of this, including the comment "systems usually are obsolete and need to be replaced within 3-5 years - this one has already outlived it's lifespan by 5".

Last I heard, they're still running effectively the same stuff.... (10 years later)

Chris Lewis, Elegant Communications Inc., Markham, Ontario, Canada, {uunet!attcan, utzoo}!lsuc!{gate!eci386, ecicrl}!clewis

#### re: Structured Programming

John (J.G.) Mainwaring <CRM312A@BNR.CA> 20 Jan 89 16:16:00 EST

In the replies to Karsh's article published to date, several interesting points were made, but one clear statement of objective was missing. The methods which have come to be known as structured programming were intended to avoid the use of what were then recognized as error prone contructs. This is in the spirit of analyzing aircraft accidents and changing instrument or control designs which pilots tended to misunderstand or misuse.

There may well be those who have lost track of the idea that the structuring of a program should break the job down into segments which are small enough to understand, and eliminate hidden interactions between segments which make it difficult to understand how they fit together. It is possible to indent beautifully, avoid gotos, keep modules under a page, and use data structures that make it totally impossible to understand how it all fits together. The larger the system, the greater the difficulty of creating an overall design and ensuring that the parts really fit together in an understandable way, ie that a structure really exists at ALL levels.

Does anyone know of recent studies based on current languages used in nominally structured fashion of what errors are most common and what disciplines seem most likely to avoid them? Such articles used to be common at one time. Perhaps now would be a good time for a few more, preferably in some of the popular as opposed to academic magazines. The converted may enjoy a good sermon, but it has the chance to do more good when it reaches a wider audience.

My views are probably my own but only coincidentally those of my employer or anyone else.

## Structured Programming, Object Oriented Programming: A quote

Mark Rosenstein <rosenstein@mcc.com> Sat, 21 Jan 89 08:27 CST

David A. Moon from the foreword to "Object-Oriented Programming in Common Lisp" by Sonya E. Keene [an interesting book, by the way]:

The nature of object-oriented programming is such that it is most beneficial for large programs that are written by multiple authors and are expected to last a long time. The ease of implemententing a small, simple program does not much depend on what programming methodology is employed, and one who has dealt only with small programs may not see any point to the object-oriented discipline. However, anyone who has been through the design, development, documentation, testing, and maintenance of a large software system in a non-object-oriented fashion, and then has experienced the same process in an object-oriented system, will understand why there is so much interest in object-oriented programming. It isn't magic, but it is a good technique for organizing large software systems and making them comprehensible.

I believe the above is also exactly true with respect to structured programming. Mark.

## Specious Arguments and Structured Programming

Steve Pozgaj <ames!uunet!dmnhack!dmnboss!steve%pasteur.Berkeley.EDU@ucbvax.Berkeley.EDU> Fri, 20 Jan 89 08:55:40 EST

I have always enjoyed controversial debate, \*but\*, there is a major difference between controversial debate and provocation. I must say that I find Bruce Karsh's posting in <u>RISKS 8.8</u> simple provocation. It is the kind of statement that forces a "bite your tongue and count to 10" reaction. Why?

Provocation can only lead to "heat" in arguments, not "light". In this regard, I agree wholeheartedly with Jim Horning's subsequent reply that we'd all be better off, if we're to discuss structured programming, having a discussion based on "light" issues, not "heat" issues. You know, I'd bet Karsh had his tongue just about puncturing his cheek when he wrote his piece. Surely he can't have been serious? Either that or he's never produced code bigger than a student programming assignment. (Wonder how it passed with all those left-margin aligned GOTO's?-)

In the real world of programming, systems are often very complex, as well as complicated. To not bring a disciplined attitude to their construction is suicide. I learned structured programming at University, from people such as Jim Horning. It is one of many disciplines. It works, as do others. In my opinion, it works better ... but, maybe, not for everybody. However, I cannot imagine program construction without \*some\* discipline.

In any case, I view Karsh's provocation as one of "form", not "substance". He argues [very speciously] about indenting, variable naming, and other "rules" which all pertain only to form. This is like attacking literature based on rules of grammar (e.g. saying that only "free form" prose is valid poetry and that rhyming couplets produce garbage). Why waste the time? Any conclusion can be drawn from incorrect premises, which is exactly what Karsh does. By stating that SP isn't about correctness, but about maintainability, he goes on to draw all sorts of silly conjectures. So what? [...]



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 8: Issue 14

## **Tuesday 24 January 1989**

#### Contents

Re: Medical Software -- testing and verification

**Dave Parnas** NSA and the Internet

Vint Cerf

Re: Losing systems

**Geoff Lane** 

Computing Projects that Failed

**Dave Platt** 

Re: Object Oriented Programming

Benjamin Ellsworth

Losing Systems

**Henry Spencer** 

Computer Emergency Response Team (CERT)

Brian M. Clapper

Probability and Product Failure

**Geoff Lane** 

Probabilities and airplanes

Robert Colwell

Mike Olson

**Dale Worley** 

Info on RISKS (comp.risks)

## ★ Re: Medical Software (Are computer risks different?) (RISKS-8.7)

Dave Parnas <parnas@qucis.queensu.ca> Mon, 23 Jan 89 07:48:13 EST

In his contribution to Risks 8.7 Jon Jacky makes the statement that the problems of testing and verification are broadly similar whether the machine includes a computer or not. I have heard this argument from many "old-time" engineers and consider it quite false. In the testing of conventional (analog) devices we make use of the fact that the functions are continuous and that one can put an upper bound on the derivatives or the frequency spectrum. We use those mathematical properties in deciding how many tests are required to

validate a device. When digital technology is involved there are no limits on the rate of change. Further, with digital technology, the number of tests required for black-box testing increases sharply with the lowest known upper-bound on the number of states in the device. If we do "white-box" testing, we can reduce the number of tests required by exploiting the regularity of the state space. In practice, the regularity is present and helpful for the testing of hardware but not terribly useful for software testing. In short, the technology being used does make a big difference in testing and validation.

While I agree with Jon's statement that industry practices in software development are often much worse than for other kinds of technology, that is not the only explanation of our "special problem". The technology itself is a great contributor and always will be.

David Parnas, Queen's University, Kingston Ontario

#### NSA and the Internet

<CERF@A.ISI.EDU> 23 Jan 1989 01:11-EST

John Gilmore asks why NSA has 5 IMPs if they are NOT monitoring the Internet. So far as I know, NSA does not have 5 IMPs on the Internet. It has one to support Dockmaster. The agency has a variety of internal networks, of course, but none are likely to be linked to the Internet since they are used for classified applications for which the Internet is not approved.

Does Mr. Gilmore have some evidence he wishes to present that suggests the NSA is engaging in an unacceptable activity on the Internet?

Vint Cerf

VIIIL CEI

## Re: Losing systems

"Geoff. Lane. Tel UK-061 275 6051" <ZZASSGL@CMS.UMRCC.AC.UK> Mon, 23 Jan 89 09:34:58 GMT

In my experence the single most probable cause of a software project failing is that the people who started the project have no real idea what they want in the end. Almost everything else can be coped with but when you have to deal with a constant stream of "design changes" not even the best people with the best equipment can succeed.

Geoff. Lane, UMRCC

## Computing Projects that Failed

Dave Platt <dplatt@coherent.com> Mon, 23 Jan 89 10:28:18 PST On the subject of computing projects that failed for one reason or another: I recommend that interested Risks readers look up some of Bob Glass's books on this subject. Glass has collected quite a number of case-studies, changed the names to protect the innocent [and the guilty, too], and organized them into categories according to the primary reason for the failure (immature technology, wrong technology, mismanagement, misimplementation, politics, etc.). Some of the stories are roaringly funny... f'rinstance, the mainframe at "Cornbelt U." that survived a series of mishaps during installation (including being watered by the University's lawn sprinklers), only to end up destroying itself (and most of the building) during an earthquake.

Glass has written half-a-dozen books on the computing industry (most of them date back to the '70s and early '80s). The three most applicable to Risks issues are: "Computing Projects that Failed", "Computer Messiahs: More Computing Projects that Failed", and "Computing Catastrophies". [I may be off a bit in the exact wording of the titles; my copies are at home.]

Based on the recent contributions to Risks concerning recent softwareproject failures, it sounds to me as if most of the pitfalls that Glass wrote about back in the '70s are alive and well in the late '80s!

Dave Platt FIDONET: Dave Platt on 1:204/444 VOICE: (415) 493-8805 UUCP: ...!{ames,sun,uunet}!coherent!dplatt DOMAIN: dplatt@coherent.com USNAIL: Coherent Thought Inc. 3350 West Bayshore #205 Palo Alto CA 94303

#### Re: Object Oriented Programming

Benjamin Ellsworth <ben%hpcvlx@hp-sde.sde.hp.com> Mon, 23 Jan 89 13:54:59 pst

Recently a professor from the local university taught a class on OOP at our site. During the first lecture, he said that via OOP one can add functionality to the module without changing the code. I asked incredulously, "Without changing \*any\* code?" He said, "Yes." A manager at the class sagely nodded his head.

I should hope the risks are obvious.

## re: Losing Systems

<attcan!utzoo!henry@uunet.UU.NET> Tue, 24 Jan 89 02:20:32 -0500

>The losing systems almost always contain some elements of newness; in fact on >close inspection they usually contain several such elements...

To quote from John Gall's SYSTEMANTICS: "A complex system that works is invariably found to have evolved from a simple system that worked." So perhaps it's not so surprising that a lot of these done-yet-again-from-

scratch systems (how many different county records systems does the world NEED?!?) fail.

Henry Spencer at U of Toronto Zoology uunet!attcan!utzoo!henry henry@zoo.toronto.edu

#### Computer Emergency Response Team (CERT)

Brian M. Clapper <clapper@NADC.ARPA> Tue, 24 Jan 89 10:18:01 EST

Excerpted from UNIX Today!, January 23, 1989 (reprinted without permission)

WASHINGTON -- The federal government's newly formed Computer Emergency Response Team (CERT) is hoping to sign up 100 technical experts to aid in its battle against computer viruses.

CERT, formed last month by the Department of Defense's Advanced Research Project Agency (DARPA) ... expects to sign volunteers from federal, military and civilian agencies to act as advisors to users facing possible network invasion.

DARPA hopes to sign people from the National Institute of Science and Technology, the National Security Agency, the Software Engineering Institute and other government-funded university laboratories, and even the FBI.

The standing team of UNIX security experts will replace an ad hoc group pulled together by the Pentagon last November to deal with the infection of UNIX systems allegedly brought on by Robert Morris Jr., a government spokesman said.

CERT's charter will also include an outreach program to help educate users about what they can do the prevent security lapses, according to Susan Duncal, a spokeswoman for CERT. The group is expected to produce a "security audit" checklist to which users can refer when assessing their network vulnerability. The group is also expected to focus on repairing security lapses that exist in current UNIX software. To contact CERT, call the Software Engineering Institute at Carnegie-Mellon University in Pittsburgh at (412) 268-7090; or use the Arpanet mailbox address cert@sei.cmu.edu.

## Probability and Product Failure

"Geoff. Lane. Tel UK-061 275 6051" <ZZASSGL@CMS.UMRCC.AC.UK> Mon, 23 Jan 89 09:17:33 GMT

Unfortunately, from reports here in Britain after the M1 plane crash, it appears that there is a real problem with "Common Mode" failures in aircraft engines. So if one fails then the probability of a second failing during the same flight is much higher than would be expected. The probabilities of failure are not independent.

(BTW - in "fly by wire" systems they attempt to avoid common mode errors in the software by having three independent groups implementing the system on three

different types of processor. Firstly this does NOT eliminate the problems of errors in the system specification from which all three designs are derived. Secondly what happens 10 years later when the software is updated to incorporate new developments - are three more independent software houses commissioned to produce the new software - or would this be done in-house by some part-time students?)

Geoff Lane UMRCC.

## ✓ Probabilities (Re: RISKS-8.12)

Robert Colwell <mfci!colwell@uunet.UU.NET> Sun, 22 Jan 89 14:20:00 EST

There is a definite danger to this analysis, stemming mostly from its essential correctness. There was a plane within the last two years (if memory serves) that lost all three of its engines on a flight precisely because such events are not necessarily independent. Turned out that the same mechanic had worked on all three and made the same mistake on all three (left off an oil seal, I think). Another example is the nuclear reactor fire of a couple of years ago, where all the redundant control wiring was for nought because somebody routed them all through the same conduit, so they were all destroyed at the same time.

One must be extremely careful with abstract analyses like these -- they can be seductive, and they can lead to unjustified conclusions.

#### real discrete probability and airplanes

Mike Olson <mao@blia.UUCP> 23 Jan 89 10:05:05 PST (Mon)

as at least two people have pointed out, my analysis of the likelihood of failure was wrong. i claimed that the probability of two engines failing out of three was  $6(p^{**2})$ ; the correct answer, of course, is  $3(p^{**2})$ .

thanks to A. Lester Buck (siswat!buck) and LordBah@cup.portal.com for pointing out my error in a way befitting the kinder, gentler nation we now live in. it's not quite clear what i was computing, but it certainly wasn't probability. it wasn't even conditional probability, since i got the independence argument wrong.

it's important to remember one of the real risks of the network -- the potential for embarassing yourself in front of hundreds (thousands?) of intelligent people. next time, i check my work.

mike olson, britton lee, inc.

...!ucbvax!mtxinu!blia!mao

[Also noted by Mike Wescott (m.wescott@ncrcae.Columbia.NCR.COM) and Dale Worley. PGN]

## **✓** Probability

Dale Worley <worley@compass.UUCP> Mon, 23 Jan 89 10:11:29 EST

Actually, given that the probability of an engine failing during the trip, year, etc. is p, and the probability of it not failing is q = 1 - p, then:

the probability of 0 engines failing is  $q^{**3}$  the probability of exactly 1 engine failing is 3 p  $q^{**2}$  the probability of exactly 2 engines failing is 3 p\*\*2 q the probability of all 3 engines failing is p\*\*3

Given (we hope!) that p is very small, q is essentially 1, then p  $<> p^{**2} <> p^{**3}$ , so we can approximate:

The probability of (at least) 1 engine failing is 3 p . The probability of (at least) 2 engines failing is 3  $p^{**2}$ .

The trouble with "the probability of one engine failing is ... and the probability of one of the remaining two failing is ..." is that is double-counts the failures, for instance the probability of engine A failing, \*then\* engine B is approximately 1/2 p\*\*2, not p\*\*2 as assumed by the previous poster -- the other 1/2 p\*\*2 times, engine B fails before engine A.

Dale Worley, Compass, Inc.

compass!worley@think.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 8: Issue 15

## Wednesday 25 January 1989

## **Contents**

More video piracy

**Dave Curry** 

Computerized records of employee informers

**Mike Trout** 

Censorship and computers

**Anthony Finkelstein** 

Re: Object Oriented Programming

Benjamin Ellsworth

Structuring large systems

John Spragge

About non-redundant redudant systems

Elizabeth D. Zwicky

Engine-count and the Spirit of St. Louis

Michael McClary

Counting engines

Jordan Brown

Re: Space shuttle computer problems, 1981--1985

**Henry Spencer** 

Revised Computer Ethics Course Proposal

**Bob Barger** 

Info on RISKS (comp.risks)

## More video piracy

davy@riacs.edu <Dave Curry> Wed, 25 Jan 89 08:29:47 -0800

Taken from the San Jose Mercury News, Jan. 23, 1989.

Video pirates disrupt Super Bowl broadcast on L.A. cable system

LOS ANGELES(AP) - Cable television viewers of the Super Bowl said video pirates disrupted the audio portion of the play-by-play Sunday with music from "The Jetsons" cartoon show and an anti-Semitic slur.

"First there was music from 'The Jetsons' cartoon show. Then someone said something about Century Cable and 'There's too many (expletive deleted) Jews in this industry," said Doug Debber, a viewer in Santa Monica. [....]

The interruption occurred about 3:15 p.m., when an audio signal invaded Century's cable system, he [Bill Rosendahl, a company spokesman] said. Viewers in West Los Angeles, Santa Monica and Beverly Hills reported the intrusion, Rosendahl said. [.....]

Company officials have contacted the FBI and Santa Monica police and were planning to contact the Federal Communications Commission Monday morning, he said.

## Computerized records of employee informers

Mike Trout <miket@brspyr1.brs.com> 25 Jan 89 16:15:59 GMT

The 16 May 1988 issue of \_Flagship\_News\_ (employee publication of American Airlines) includes a small article on a spiffy way for employees to rat on their fellow workers. It's part of a nationwide computerized database on "business abuse," which is apparently a euphemism for workers who don't measure up to management's standards. Listed examples of business abuse include theft, drug and alcohol abuse, unsafe work habits, and "any act not in the best interest" of the employer. All you have to do to destroy your fellow workers is call the National Business Crime Information Network Inc. (known as "The Network"), at 1-800-241-5689. You may do this anonymously, as each caller is simply assigned a code number. This also allows you to call back later and check to see what action has been taken against that guy in the next cubicle who took a pencil home. The Network says that your information is relayed to top management, who it is claimed will not take any disciplinary action on the basis of the phone call alone.

Right. Michael Trout
BRS Information Technologies, 1200 Rt. 7, Latham, N.Y. 12110 (518) 783-1161

[If you make your ratfink call from a phone with automatic calling identification, do they store YOUR phone number as well? PGN]

#### Censorship and computers

<acwf@doc.imperial.ac.uk> Wed, 25 Jan 89 12:02:54 GMT

The following is taken from an advertisement which appeared in The Spectator (a conservative review and comment journal of high repute) 14 Jan 1989. The advertisement was placed by INDEX ON CENSORSHIP a magazine which publishes banned literature from all over the world, factual reports on writers and journalists who have been silenced, as well as comment, interviews and a country-by-country chronicle of censorship.

"Dear Spectator Reader,

Vaclav Havel, the well known Czechoslovak playwright, had his personal computer/word processor confiscated by police on 27 October 1988. I wonder if you would like to join with others in providing him with a replacement?

Havel had the computer for just over a year and had been using it - for work and correspondence for only a month or two. It was obtained perfectly legally. He has written to the authorities to ask for his property back, but it has not yet been returned, nor is there any sign that it will be.

The letter continues by requesting contributions for a replacement. This is of interest reflecting the risk that computers pose to oppressive states, the risk of confiscation by the police of a vital tool of modern work and communication.

Anthony Finkelstein, Imperial College of Science, Technoloy & Medicine (University of London). UK.

[I imagine replacements would be confiscated even more quickly, especially if more continue to arrive. The police may be developing a taste for computers. Besides, they may have discovered that the storage provides a convenient record of what he has written. I wonder whether Glasnostradamus predicted things like this. PGN]

## ★ Re: Object Oriented Programming (Risks-8.14)

Benjamin Ellsworth <ben%hpcvxben@hp-sde.sde.hp.com> Wed, 25 Jan 89 9:23:17 PST

[Regarding adding functionality without changing the code:]

- > I should hope the risks are obvious. [Ellsworth, RISKS-8.14]
- <>MBR@PELICAN-SPIT.ACA.MCC.COM [Message to Ellsworth and RISKS]
- <>from "Mark Rosenstein" at Jan 25, 89 6:07 am
- <> ...Oh dear. They're not obvious to me. If change means modify existing
- <> code, then I can't quite see the problem, if change means add code,
- <> yep you'll have to add code to get more functionality. Mark.

To detail the exchange seems to me to be a bit maudlin, so let me just say that we were talking about adding/changing functionality to an object. The professor's statements were cleary pointed toward no change neccessary to the code comprising the object.

#### The risks are:

Merely parroting the party line (OOP eliminates changes to operational code), and not thinking carefully about the question.
 This seems especially dangerous when instructing the empowered naive. There were managers and engineers who were receiving their first exposure to OOP in that class. They were going to try to use the information from that class in real products.
 Their (the empowered naive) perceptions and beliefs are soon going to effect other people's lives.

- Management hearing the party line and accepting a "panacea" type solution. This is an "oldie-but-goodie" (maybe even in the all-time top ten) in the category of "Engineer's Gripes," and it's currently getting a thorough flogging in RISKS.

The above in no way reflects the views of Hewlett-Packard Company.

Benjamin Ellsworth ben%hp-pcd@hp-sde.sde.hp.com

[There are indeed lots of ways to get a program to do something else without modifying the code. Moving it from one directory to another can have all sorts of side-effects, especially in a system with search strategies. Not moving it but altering the search strategy for subtended programs is another way. Redefining parameters, abbreviations, user profiles, etc., is another. How about inadvertent effects resulting from someone else innocently introducing an operating system change? All of this relates to the old saw about hardware degrades but software does not. Not true. PGN]

## Structuring large systems

<John.Spragge@QueensU.CA> Wed, 25 Jan 89 17:08-0500

By all means, we need new structures. There's no question about that. The only question is, what should we build those new structures on?

I believe that the problem of relating the behaviour of a program to it's (human-readable) static representation has been solved at a "micro" level. And, pace the disbelievers in structured programming, I believe that structured techniques represent the best solution at the procedure level. The question is the a matter of tying a large number of procedures into a workable, consistent, large system.

The answer to that, it seems to me, is to envisage the system as a machine (needless to say, programs are, in the strict sense, machines in the same way computers are). The starting point for fulfilling the requirements of an end-user who wants a particular software product is to ask what sort of "special purpose" computer would be best at solving that problem. The program can then be structured as an attempt to simulate that system on a general-purpose computer.

For example, a good analogy for writing a spreadsheet would probably be a large array (or "matrix") processor, in which every cell could simulate a "processor" having access to a central series of processing functions. A windowing system can be written as an "ideal" terminal device.

This approach has the advantage of encouraging the same sort of "generality" in design that computer hardware benefits from; the adders on a system generally work because the system has just one general purpose adder, not a vast series of different adders. In the same way, a wide variety of the functions in a system which appear to be very different share many (if not most) critical

attributes, and sufficiently flexible routines can be devised, in many cases, to apply to all the disparate functions required.

This is only one approach to the "larger" structure of systems design. But when building a large building, it does no good at all to discard the girders.

Orthodox "structured" programming techniques are, I am convinced, at the heart of building reliable procedures, without which no large system can be built. It isn't possible to build a giant program on nothing but the knowledge of Ifs, Whiles, and Cases; but they are essential components of good programming.

John G. Spragge, Computing Consultant, Box 2042, Kingston Ont. (SPRAGGEJ@QUCDN)

## About non-redundant redudant systems (Re: RISKS-8.14)

Elizabeth D. Zwicky <zwicky@cis.ohio-state.edu> Wed, 25 Jan 89 11:14:04 EST

Of our many computer rooms and labs, 2 have redundant air-conditioning systems. One of them has two separate systems installed at two completely different times by two different companies; it gained redundancy out of necessity because the first air conditioner barely had the capacity. The second one started out with two air conditioners, because it seemed like a good idea. They were installed at the same time, by the same company. Less than a month later, that room started getting hotter and hotter and hotter. We called A/C repair. They said they would log it as non-emergency, due to the second A/C in the room. We pointed out that the second A/C was not air conditioning any more than the first was. They grudgingly updated it to an emergency call, and in short order one of Ohio State's people arrived. 5 minutes later he developed an amazed/ appalled look, and began to curse. "What the hell sort of a redundant system is this? What do those jerks think they are playing at?" It seems that our two A/Cs had but one thermostat, which had duly failed. Needless to say, Ohio State made all sorts of grief for the vendor, who eventually managed to make the systems more redundant. Nevertheless, reliability is \*still\* higher in the cobbled-together, afterthought-redundant system, than in the "properly" designed one.

Elizabeth D. Zwicky, Ohio State University Computer and Information Science

## Engine-count and the Spirit of St. Louis

Michael McClary <xanadu!michael@uunet.UU.NET> Sat, 21 Jan 89 01:29:46 PST

The more-is-less phenomenon of aircraft engine reliability has been noted previously.

During the push to extend aircraft technology to non-stop trans-Atlantic flight, most of the designs were multi-engined. The designers of the Spirit of St. Louis recognized:

- they were on the edge of the technology, therefore

- there was insufficient spare capacity to carry a dead engine, and
- there was nowhere to land for repairs, therefore
- all the engines would have to run for essentially the whole flight, so
- assuming roughly equal engine mean-time-to-failure, the more engines, the greater the risk of failure (with loss of craft and pilot).

Thus the Spirit of St. Louis was designed with a single engine.

It's a classic examples of the counter-intuitive nature of probability theory and risk assessment.

(Of course, practical service had to wait a bit, until aircraft capacity and airport availability improvements made single-engine-failure survivable.)

## Counting engines

Jordan Brown <jbrown@herron.UUCP> <jbrown@jato.Jpl.Nasa.Gov> Sun, 22 Jan 89 19:55:01 PDT

Don Alvarez <boomer@space.mit.edu> writes:

- > Imagine two planes which are identical except that one plane has 2
- > Bratt&Zittley Foobar-900 engines, and the other has 3 B&Z F-900 engines.
- > Well, clearly the second will fly better on n-1 engines, ...

This is the misconception that I'm trying to point out. If you have an airplane which flies fine on two B&Z F-900s (meets single-engine performance requirements, etc) then no manufacturer would ever put another engine on that airplane. It just wouldn't make sense. (This is for civilian applications; military apps have other issues.) The three-engine airplane discussed will either be bigger or have wimpier engines. The controlling factor is engine-out performance. The two-engine airplane with one out will have performance comparable to the three-engine airplane with one out.

727 engines (3/airplane) are wimpy compared to DC-9 engines (2/airplane). BAe-146 engines (4/airplane) are \*really\* wimpy. (This assumes that 727s are approximately the same size as DC-9s. Bae-146's are smaller.)

Jordan Brown

#### ★ Re: Space shuttle computer problems, 1981--1985

<attcan!utzoo!henry@uunet.UU.NET> Tue, 24 Jan 89 00:25:52 -0500

>STS-6, April 4, 1983: ... Landing gear must be manually deployed after computer >fails to trigger its descent.

I wonder if this is not mistaken reporting at some level. My recollection, possibly incorrect, is that lowering of landing gear is specifically not under computer control in the space shuttle -- it \*has\* to be done manually. The reason is that once lowered, the shuttle's landing gear is \*down\* --

it can't be raised again in flight.

Possibly the problem was that the computer did not say "time to lower the gear"?

Henry Spencer at U of Toronto Zoology

uunet!attcan!utzoo!henry henry@zoo.toronto.edu

### Revised Computer Ethics Course Proposal

Bob Barger < CFRNB@ECNCDC.BITNET> Wed 25 Jan 1989 09:34 CDT

The following revision is based on critiques received on a proposal published in RISKS digest 7.75. Comments are still welcome (send to CFRNB@ECNCDC.BITNET). Course Description: The course will investigate current ethical issues involving computers. While it is not a "computer course," students will make frequent use of postings on the electronic bulletin board of the ECN mainframe computer to research and discuss ethical issues. Prerequisites: 75 Semester Hours and previous experience with computers. [Class size limit = 15 students for Fall, 1989, semester]. Outline of topics: Week 1: Orientation to the course (introduction, explanation of course content, class procedures, and evaluation methodology). Consideration of ethical theory. Week 2: Consideration of ethical theory (continued). Week 3: On-line reading of the "Discussion of Ethics in Computing" list, the "Forum on Risks to the Public in Computers and Related Systems" digest, and the "Computers and Society" list (all are available on the ECN bulletin board); written reactions to these readings, and written commentary on other students' reactions. [The instructor will insure that these activities equate to the activities of a traditional two hour class meeting]. Week 4: Consideration of professional ethics. Week 5: Same activities as for Week 3. Week 6: Consideration of liability for software design, manufacture, and use. Week 7: Same activities as for Week 3. Week 8: Consideration of privacy issues. Week 9: Same activities as for Week 3. Week 10: Consideration of power/control issues. Week 11: Same activities as for Week 3. Week 12: Consideration of ownership and theft issues. Weeks 13 & 14: Same activities as for Week 3. Week 15: Seminar members will reconvene as a group for the last meeting to allow for group reflection on the seminar experience and course evaluation. Semester Exam week: Final Examination. Writing component: Students will type thirteen 30-to-50 line (i.e., one-to-two page) reactions to the on-line electronic bulletin board readings. Students will "post" these reactions (i.e., electronically send them to the mainframe computer bulletin board set aside for members of this seminar). In their reactions, students will: 1) identify the particular publication or publications to which they are reacting, 2) identify the particular issue or issues raised in the publication(s), 3) identify the ethical implications of the issue or issues, 4) identify the ethical paradigm used by the author, 5) add their own reasons for agreement or disagreement with the viewpoint of the publication's author, 6) and, finally, offer an alternative solution or viewpoint to that presented by the author, or present other appropriate considerations not raised by the author or covered in their own (i.e., the student's own) previous comments. The instructor will send weekly, by confidential electronic mail, a grade on the student's posted reaction, together with whatever comments the instructor thinks helpful. The student's original posted reaction will also be open to public comment by the other students in the seminar [this is accomplished by

posting notes to the bulletin board, referencing the original posted reaction]. These latter comments by the other students in the seminar will be considered along with classroom discussion in computing the "participation" factor of the student's semester grade. Evaluation: Each student's semester grade for the seminar will be calculated according to the following weighted formula: 13 posted reactions (at 5% each) = 65%; Participation (based on class discussion and posted comments on other students' reactions) = 20%; Final Exam = 15%. Materials in the course will include: 1) Texts: Deborah Johnson, Computer Ethics (Englewood Cliffs, NJ: Prentice Hall, 1985); privately published notes on systematic ethics from Dr. Barger's Philosophy 1800 class (furnished free to seminar members); postings on the above-mentioned ECN electronic bulletin board lists. 2) Resource people: Computer professionals (e.g., administrators, systems analysts, programmers, etc.) will be utilized as guest contributors to the class. This will be accomplished by personal appearances, as well as by electronically mediated conferencing (e.g., postings, e-mail, relay round-tables, etc.).



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 8: Issue 16

## Thursday 26 January 1989

## **Contents**

Cable video piracy

anonymous

F-111 downed by EMI?

**Gordon Davisson** 

F-16 that can't stall falls from sky

Mike Tanner

Re: Probability and Product Failure [common mode failures]

**Bruce Hamilton** 

Discrete probability and airplanes

**Dave Settle** 

Micro-cellular phones

Steven C. Den Beste

Looking for Computer Folklore Karla Jennings via Vernard C. Martin

Info on RISKS (comp.risks)

#### Cable video piracy

<[anonymous]> Wed, 25 Jan 89 18:40:10 PST

Subject: Century Cable video "pirate" [RISKS-8.15]

It appears likely that this was not truly a case of piracy, but rather an "inside job" of employee sabotage.

There are some pretty good reasons for suspecting this:

1) The content of the audio. It consisted of one voice introducing the next as a person who is a manager/executive at Century cable. The name used was indeed an actual person at Century, but of course that person himself was presumably not actually involved. The introduced voice did a pretty poor Reagan imitation, by the way.

2) Technical evidence. On the channel of the superbowl, and ONLY that channel, the normal audio was cleanly removed and replaced with the offending audio. Without going into technical detail, it would be extremely difficult to REPLACE the audio on only one channel of the cable (through the cable itself) without interfering with other channels and in general disrupting other channels at least for short periods. To replace audio requires a full demodulation/re-modulation, not just a "simple" RF insertion into the RF of the cable.

The most likely point for insertion of the audio was WITHIN the cable company headend itself, where each channel video and audio is individually modulated onto the cable. This would require physical access to the inside of the headend facility.

3) Century Cable has been having labor difficulties (note the use of a company manager's name in (1) above).

#### ✓ F-111 downed by EMI?

Gordon Davisson <gordon@june.cs.washington.edu> Thu, 26 Jan 89 00:26:04 PST

Copied without permission from the Seattle Times, Jan. 20, 1989:

by Mark Thompson, Knight-Ridder Newspapers

WASHINGTON -- When U.S. warplanes were ordered to strike Libya in 1986, they ran into an electronic blizzard the Pentagon now suspects might have caused one of the fighters to crash and others to miss their targets.

The disruption came not from the Libyans but from U.S. military transmitters that filled the night sky with electronic signals designed to jam Libya's anti-aircraft defenses, hunt down targets, guide weapons and communicate.

The Pentagon is so alarmed by the problem that it has launched a \$35 million effort to identify the interference and keep it from happening again, according to Air Force Col. Charles Quisenberry, who is leading the probe.

During the Libyan strike, U.S. weapons "were interfering with each other, and they (U.S. commanders) came back out of that and they said: 'Look, we've got some problems here, and we want to know if we're doing it to ourselves, or if the bad guys did it to us,'" Quisenberry said in an interview. "The end result was we found out we did it to ourselves."

President Reagan ordered the April 1986 strike after U.S. intelligence linked Libya to the terrorist bombing of a West German nightclub in which an American serviceman was killed.

Quisenberry said the radiowave interference might have lead to the downing of an F-111 warplane, whose two crew members were the only U.S. fatalities in the attack. "It could have," he said. "We couldn't rule it out or say that that was the cause."

Last Friday, Libya returned the body of one of the fliers, Maj. Fernando Ribas-Dominicci of Utuado, Puerto Rico. The body of the other pilot, Capt. Paul Lorence of San Francisco, is still missing.

Numerous U.S. weapons, some of which were electronically guided, went astray during the attack, damaging three foreign embassies and diplomatic residences, including those of France and Japan. Seven of the 32 remaining planes -- including five F-111s -- aborted their missions without firing a shot because of unspecified problems.

Recent Pentagon studies have shown that some combinations of U.S. weapons transmitting at certain frequencies can bring down American warplanes, Quisenberry said. "Some are very, very critical -- some cause aircraft to crash."

Quisenberry recently finished a classified seven-month investigation of the problem, which led top Pentagon officials to order the new investigation.

Research may yield embarrassment, Quisenberry acknowledged. "Many people have told us that a lot of people will not be happy with what we find out because we'll actually uncover problems," he said. "If there's a problem with the B-1 that might not be politically acceptable, people may have some heartburn with that." In the past, Quisenberry said, the Pentagon too often has ignored its own safeguards designed to protect weapons from electromagnetic interference. "EMI just got a low priority," he said.

"In many cases, a program manager will get an exemption for getting a weapon delivered without having EMI (electromagnetic interference) looked at completely," Quisenberry said.

The havoc radio waves can cause was first made public in 1987, when Knight-Ridder reported that some Army safety officials believe the phenomenon was responsible for up to five crashes of the Army's UH-60 Black Hawk helicopters that had killed 22 servicemen since 1982.

[The Blackhawk problem was discussed in RISKS-5.56,58,59,60 and 7.8,9 -- GD]

Gordon Davisson (gordon@june.cs.washington.edu) (uw-beaver!uw-june!gordon) Computer Science Department, University of Washington. Seattle, WA, 98195.

## ✓ F-16 that can't stall falls from sky (RISKS-8.13)

Mike Tanner <tanner@cis.ohio-state.edu>
23 Jan 89 23:11:12 GMT

This may not be a risk of computers, but maybe a risk that arises from reporting technical subjects in the popular press -- inaccuracy.

Airplanes can be stalled in any attitude (angle with respect to the ground) at any airspeed. So I'm puzzled about this:

> The F-16 can stall at speeds of 230 mph or slower, depending on its weight > and angle of flight, MacDill officials said.

It might mean that below 230 the computer anti-stall stuff doesn't work. Though I can't see why it should be related to speed. Stall is a function of angle of attack, not of airspeed. There is a certain speed (called maneuvering speed in light airplanes, don't know about fighters) beyond which the airplane will be damaged by a stall. So maybe 230 is this speed for the

F-16. That is, below 230 it's a stall, above 230 it's an in-flight breakup.

Then there's this:

> The report drawing depicts Johnson's jet in a near-vertical climb just before > it stalled. "That should never have happened," said Howard Acosta

Since Acosta is said to be an experienced pilot I assume "That" refers to the stall, not the vertical climb. Though the latter is implied by the context. Again, stall is a function of angle of attack, not attitude (i.e., angle with the ground). Some reporter believes, or was led to believe, that "stall" is caused by an extreme nose-high attitude.

Anybody know how the F-16's anti-stall stuff really works?

-- mike

## Re: Probability and Product Failure [common mode failures]

<"Bruce\_Hamilton.OsbuSouth"@Xerox.COM> 26 Jan 89 13:11:50 PST (Thursday)

It's worth pointing out that common mode failures in software go beyond the system specification -- programmers tend to make similar sorts of errors way down in the implementation, even in so-called "independent" implementations.

Re: aircraft-specific common mode failures: exhausted fuel has happened within the past two years; contaminated fuel would be another example. I'm sure an aircraft engineer could come up with dozens of other possibilities.

--Bruce UUCP: xerox.com!hamilton.osbuSouth 213/333-8075

## Discrete probability and airplanes

Dave Settle <dave@ucms.UUCP> Wed, 25 Jan 89 11:46:16 GMT

In <u>RISKS 8.10</u> Steve Jay <shj@ultra.com> comments:

- >> Even assuming that a 3 engined plane needs 2 engines to fly,
- >> the odds of 2 engines failing on a 3 engined plane are much, much
- >> smaller than the odds of 1 engine failing on a 2 engined plane.

Not true. It is MORE likely to happen.

In RISKS 8.12 Mike Olson <mao@blia.uucp> comments:

> If the probability of 1 engine failing is p, then the probability of one > of 3 engines failing is 3p ...

Not true either. [ if 'p' is a probability, then '3p' isn't: suppose p = .5?] (mind you, you wouldn't sell many of them :-)
[Wrong. `3p' is an approximation that is perfectly good for small p. PGN]

To put things straight about probabilities: (assuming that the 2-engine plane needs 1 engine to fly, and that the 3-engine plane needs 2)

A 2 engined plane will crash iff both engines fail - probability p^2. Call this p2.

A 3 engined plane will crash iff any pair of engines fail, or if all 3 fail together.

The probability of a pair of engines failing is p \* p \* (1 - p): i.e. FAIL FAIL OK. There are 3 DIFFERENT pairs to be considered: AB, BC, or AC.

The probability of all three engines failing is p^3.

Therefore the probability of at least 2 engines failing is:  $3p^2(1-p) + p^3 = 3p^2 - 2p^3$ . Call this p3.

p2 is the probability that the 2-engined plane will crash, p3 is the probability that the 3-engined plane will crash.

Since p < 1, p2 < p3 (that is, the 2-engined plane is safer): proof:

```
p^2 < 3p^2 - 2p^3

0 < 2p^2 - 2p^3 (subtract p^2)

2p^3 < 2p^2 (add 2p^3)

p^3 < p^2 (divide by 2)
```

which is TRUE for p < 1.

So, what does all this mean? Well, basically it's safer to use a 2-engined plane than a 3-engined plane: the 3-engined plane will crash more often, assuming that it needs 2 engines to fly.

You can sort of make sense of this by thinking that the 2-engine plane needs 50% of its engines working, while the 3-engine plane needs 66%. Of course, you could always travel by Greyhound.

Hope this makes sense (and I haven't made any mistakes :-) )

[Thanks to Martin Jeffries for help with the maths etc]

Dave Settle, Universal (CMS) Ltd, Thames Tower, Burleys Way, Leicester, UK.

```
dave@ucms.co.uk (someday) ...!mcvax!ukc!nott-cs!ucms!dave dave@ucms.uucp (today)
```

<--- This way to point of view --->

### Micro-cellular phones

<denbeste@BBN.COM>
Sun, 22 Jan 89 11:22:02 -0500

#### Excerpted from the 1/30/89 Business Week:

- "...Now the British are readying a novel mobile phone service based not on cellular technology but on cordless phones. Customers will have to place calls within range of a local transceiver, and they won't be able to receive calls. [The customer must stay near that transceiver for the duration of the call. SDB]
- "...The cordless phones will transmit signals to large transceivers tucked away in key public places and connected by wire to the regular phone network. As long as the caller is within 100 to 200 yards of a station, a call can be placed to anywhere in the world by punching in a special code and then the number.
- "...License applicants figure it will take no more than \$70 million to build a nationwide network of 20,000 base stations, placed in such busy sites as train terminals and gas stations.
- "...Initially the phones will retail for about \$275 in Britain..."
- "...Telepoint's boosters expect Britain to be a \$1.4 billion market with 4 million subscribers by 1994.
- "...British consumers soon will be able to buy a small CT2 base station [for their homes] for about \$200, and use it in place of a regular phone and expensive wiring to connect up to eight CT2 cordless handsets.
- "...On each call, a CT2 phone finds the first available frequency among 40 channels. Backers say its low power output means that up to 14,000 phones could operate simultaneously per square mile.
- "...Telepoint's backers are betting that the new service will attract enough cost-conscious consumers to turn a quid or two. [because CT2 costs much less than a real cellular system SDB]"

This takes my breath away. Are there NO paranoids in the British telephone authority?

- 1. What is to keep me from setting up a receiver in the London financial district and listening in on important calls there? [Did someone mention "inside trading"? How the heck are the authorities going to prove where I got my information?]
- 2. The "special code" I have to enter is presumably a customer ID. [If they expect an installed base of 4 million, it's probably going to be 11 digits. How much you want to bet they make the phone do it automatically?] If I put my receiver somewhere rich (the financial district again?) I should be able in very short order to capture the access codes for literally hundreds of very well-off people. All I have to do now is modify my own phone slightly, and next time I want to chat with my girl friend in Singapore for a couple of hours, there I am free long distance!

If the phone company detects something funny going on with a normal line, they know exactly where it is and can send the cops. But with one of these, all they know is approximately where it is - and a 200 yard diameter is a big place to search when you don't know what you are looking for and don't have warrants to open doors and search.

These problems are fundamental in the design. Because they will have an enormous installed base, they can't change the fundamental system at all - by

adding scramblers, for instance, or changing the tones for the keypad. Once the system is installed, I don't see what they can do to handle these problems when they pop up.

"Cost conscious consumers" indeed. If the engineering schools at Oxford and Cambridge are anything like the ones at MIT and Caltech, they're going to tear this system to shreds.

Steven C. Den Beste, BBN Communications Corp., Cambridge MA denbeste@bbn.com(ARPA/CSNET/UUCP) harvard!bbn.com!denbeste(UUCP)

## Looking for Computer Folklore

Vernard C. Martin <isusevm%pyr@gatech.edu> 26 Jan 89 01:18:40 GMT

I'm interested in stories that might have started in actual fact but that have become so popular that they keep popping up. For instance, did you hear about the zero-sum check? Someone gets a computerized bill from a credit card company saying they owe the company zero dollars and zero cents. They ignore it but keep getting bills and increasingly nasty computerized notes, so they finally write out a check for zero dollars and zero cents and send it in, and the computer never bothers them again.

Or, there's the story about the guy who falls asleep in front of his terminal with an ELIZA program running and his boss logs on and thinks he's talking to him but is actually talking to the program, and gets pissed off.

OR, there's the dilemma in which computers keep crashing because an operator wears a silk slip that gives off static electricity like nobody's business, OR the bank teller who embezzles millions from his bank by creating a file to collect the fractions of pennies that the bank rounds off from accounts.

Some story categories are:

- 1. machines going physically berserk.
- 2. women/computers/sex/sexism and/or romance.
- 3. sabotage.
- 4. breaking security (no, I don't have classified clearance [...])
- 5. great hacks.
- 6. computer gods (such as Norbert Weiner, a genius in AI who lost his family when they moved to a new house and he forgot where it was).
- 7. tales of massive catastrophe due to seemingly mysterious means that turn out to be something strange, like magnetized pollen.

Of course, there are more categories. Got a great tale you want to share? Reply to isusevm@pyr.gatech.edu. If you'd rather talk, leave your phone number and I'll try to give you a ring.

Karla Jennings

This account is temporarily being used as a collection point for mail. isusevm@pyr.gatech.edu

[The zero-dollars story appears among an old collection of anecdotes from an ACM SIGOPS Symposium on Operating Systems Principles, contained in ACM Software Engineering Notes vol 5 no 1 (Jan 1979) and augmented in vol 7 no 1 (Jan 1981). I hope our readers will share their documentable true tales (that have become legends) with RISKS as well as Karla -- especially those that have not appeared here yet. 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 8: Issue 17

# Friday 27 January 1989

# **Contents**

- ELIZA and Joe Weizenbaum
  - **Bard Bloom**
- Savings, Loans, and Easy Money
  - **PGN**
- Risks of inept management ["Losing Systems"]
  - John R. Levine
- MIT Athena Kerberos Authentication System available for FTP
  - John Kohl via Jon Rochlis
- Single-engine planes
  - Phil Karn
- Multi-engine airplanes
  - **Craig Smilovitz**
- Info on RISKS (comp.risks)

#### ELIZA and Joe Weizenbaum

Thu, 26 Jan 89 22:48:52 EST

- > Or, there's the story about the guy who falls asleep in front of his
- > terminal with an ELIZA program running and his boss logs on and thinks he's
- > talking to him but is actually talking to the program, and gets pissed off.

This may have actually happened. Joseph Weizenbaum (MIT professor, author of Computer Power and Human Reason ) told the anecdote in a class, with himself as one of the actors. It went something like this -- some of this is doubtless my own memory inventing things. The dialogue is partially courtesy of GNU Emacs' Eliza program, and the rest is made up.

Weizenbaum had recently written ELIZA on one of the MIT AI Lab's computers. In those days, computers were rather weak. The computer in question had a time-sharing system on it, yes, but it got rather sluggish when two people were using it at the same time. Weizenbaum left ELIZA running one evening and went home.

That evening (around 4 a.m.), another AI Lab person was trying to get his program working for a demonstration to his funding agency the next day, and it wasn't working very well. He was using the computer Weizenbaum was logged on to, and decided that he needed the whole thing. He went to Weizenbaum's office, hoping that he could persuade Weizenbaum to log off.

When he got there, Weizenbaum was nowhere to be found, and his terminal was on (and blank). The Alist thought that Weizenbaum was working from home, and had slaved his office terminal to his home one. So, he typed "Joe, please log off."

"WHY DO YOU SAY JOE LOG OFF?"

"I need the computer for an AI demo tomorrow, Joe"

"WHAT MAKES YOU BELIEVE THAT?"

"Joe, I'm serious. I've got a demo here tomorrow and I need the computer."

"PERHAPS THE PEOPLE YOU HANG AROUND WITH COULD HAVE CAUSED THIS."

After a few more exchanges like this, the Alist decided that Joe was being very obnoxious, and called him at home to scream at him. "Joe! You \*\*\*\*\*\*! Why are you doing this to me?"

Recall that it was four in the morning, and that Weizenbaum had no idea that his creation was running amuck in the AI lab. He quite reasonably replied, "Why am I doing \_what\_ to you?" This sounded so much like what ELIZA had been saying that it was hard to convince the Alist that it hadn't been Weizenbaum on the terminal.

#### Savings, Loans, and Easy Money

Peter Neumann <neumann@csl.sri.com> Fri, 27 Jan 1989 10:16:40 PST

Although the computer roles are probably insignificant, the scope of the abuses in the savings and loan insolvencies (estimates are approaching \$100 billion just in bail-out money) are such that upwards of 20% of the cases are alleged to involve fraud. The incentives seem rather simple -- set up an apparently legitimate S&L, make all sorts of loans to friends, let them all default, and then let the government pick up the pieces for the legitimate investors. Three of the nation's largest CPA firms -- Deloitte Haskins & Sells, Coopers & Lybrand, and Touche Ross & Co., plus smaller firms, have been sued for their roles in failing to detect fraud. Another large firm, Arthur Young, proclaimed Vernon S&L of Dallas clean shortly before federal regulators declared it insolvent -- because 90% of its loans were bad. Whatever the mixture of mismanagement, incompetence, fraud, and other factors turns out to be, the situation seems pervasive. Why were the auditors were out to lunch?

Even if the era of decontrol were ended, it seems that a such widespread problem could not be aided by better computerization (knowing what we know

about rigging computer systems, it might make fraud even easier!) -- except possibly in providing better on-line data for the auditors that might simplify their task of rectifying computer records with reality. Overall, enormous amounts of money seem to encourage fraud and creative mismanagement. Computer systems designed to withstand misuse by one user will no longer suffice. Separation of duties and the principle of least privilege help a little, but massive collusions may become the order of the day, in which case checks and balances -- even on the auditors -- become critical. Who checks the checkers?

As far as who pays, I imagine that because of the S&L incorporation rules there will be no deep pockets other than the taxpayers and S&L customers. So the real culprits will probably go untapped. But recall the advice of Deep Throat: ``Follow the Money."

# Risks of inept management, was "Losing Systems"

John R. Levine <johnl@ima.isc.com> Sun, 22 Jan 89 23:16:13 EST

In issue 12, Keane Arase details a story of a botched data collection manufacturing package at a large company which I assume to be Procter and Gamble. He reported on staff turnover, bad hiring, insufficient resources, bad design, and a host of other terrible problems. He points out that some of the trouble could be traced to bad management. It sounds to me like all of the trouble was due to bad management. Although large computing projects are often plagued by management problems, such difficulties are by no means unique to the computing business.

For example, he points out that his department was made a profit center with profits measured quarterly even though the system wasn't expected to be profitable for two years. Normally under the profit center model, separate centers are supposed to deal with each other as though they were separate businesses, i.e. the client department should be making progress payments or the computer department should have some provision for treating the progressing project as a growing asset. Accounting of multi-year projects is hardly an unknown art, the construction business has been doing that at least since the time of the Pyramids.

Finally, problems of under- or mis-specification aren't unique to the computer industry either. In New Haven CT there is (was? it may have been torn down by now) an extremely badly built pre-fab housing project called Oriental Gardens. It had no rain gutters, letting in the rain and snow to cause all sorts of damage. Why? The houses were partially constructed at a factory, then transported and assembled on-site. The factory expected the gutters to be added on-site, the on-site expected them already to be on the houses when they arrived.

The message here is that project management is a real problem, but it isn't really a technological problem except where traditional project management techniques fail to handle unique aspects of computer systems. There is a lot of management knowledge to be had for those that want it.

# MIT Athena Kerberos Authentication System available for FTP

Jon Rochlis <jon@BITSY.MIT.EDU> Thu, 26 Jan 89 22:18:39 EST

What is Kerberos and why is it needed?

In an open network computing environment a workstation cannot be trusted to identify its users correctly to network services. Software on the workstations may not be trustworthly, so being a privileged user on a workstation is not a meaningful test of authenticity. Source network addresses are so easily forged that they are are meaningful either. Passwords sent uncrypted on the network are vulnerable to wiretappers. Kerberos provides an alternative approach whereby a trusted third-party encryption-based authentication service is used to verify users' identities. Much more information is available with the documentation (see below).

How to get it:

The first public release of the Kerberos Authentication System is ready for retrieval. Initial distribution will be by anonymous FTP; eventually 9-track tapes will be available.

To retrieve the distribution, ftp to ATHENA-DIST.MIT.EDU (18.71.0.38), login as anonymous (password whatever you like, usually your username@host), then cd to pub/kerberos.

Retrieve README.ftp, it has directions on how to get to the rest of the software.

Distribution is split compressed tar files (xxx.Z.aa, xxx.Z.ab, ...).

If you would like to retrieve documents separately, you can get them from pub/kerberos/doc (documents) or pub/kerberos/man (manual pages). If you prefer hardcopy of the documentation, send your address and request to "info-kerberos@athena.mit.edu".

If you would like to be put on the Kerberos e-mail list ("kerberos@athena.mit.edu"), send your request to "kerberos-request@athena.mit.edu".

I would like to thank the following people for their assistance in getting Kerberos in shape for release:

Andrew Borthwick-Leslie, Bill Bryant, Doug Church, Rob French, Dan Geer, Andrew Greene, Ken Raeburn, Jon Rochlis, Mike Shanzer, Bill Sommerfeld, Jennifer Steiner, Win Treese, Stan Zanarotti.

FYI, the copyright notice:

Copyright (C) 1989 by the Massachusetts Institute of Technology

Export of this software from the United States of America is assumed

to require a specific license from the United States Government. It is the responsibility of any person or organization contemplating export to obtain such a license before exporting.

WITHIN THAT CONSTRAINT, permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of M.I.T. not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. M.I.T. makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

John Kohl, MIT Project Athena/Kerberos Development Team

# ✓ Single-engine planes (Re: RISKS-8.15)

Phil Karn <karn@ka9q.bellcore.com> Thu, 26 Jan 89 02:46:29 EST

My friend, Brian Lloyd, and his dad, former California congressman Jim Lloyd, flew their single engine Piper Commanche across the Atlantic from Gander to Shannon to visit the Paris Air Show a few years ago. They firmly believe that small planes with single engines are more reliable than small twin-engine planes, and they decided to demonstrate it.

Halfway across the pond, they're making one of their routine hourly position reports with a passing British Air 747. After the formalities, the following conversation ensues:

BA pilot: What're ya flying down there, 448 Poppa?

Brian: A Piper Commanche.

BA pilot: That's a TWIN Commanche, right?

Brian: Nope, single.

(long pause)

BA pilot: You're mad, you're absolutely mad, you know that! One engine?? I've got four!

Brian's dad: Well, that's just three more things to go wrong!

BA pilot: You've got me there, I've had to shut one down already!

As you can see, they lived to tell the tale...

--Phil

# Multi-engine airplanes

Craig Smilovitz <smiley@Think.COM> Fri, 27 Jan 89 09:39:26 est

In the discussion about multi-engine aircraft failures, we've seen a lot of mathematical probability exercises that forget about analyzing the basis assumption about probability theory. That assumption is the \*independence\* of the events in question.

Taking just the two engine example, everyone has been talking about the chance of a single engine failing as p. Thus the chance of an engine failing on a two engine plane is 2p (for small p, as has been pointed out). But then it has been assumed that the chance of the second engine failing is p. That would be true if the engine failures were independent. But this is not the case. A two engine plane flying on one engine is applying more stress and wear to the engine than normal (since it is probably running at close to full design capacity) Thus the chance of this remaining engine failing is more than p. How much more answers the question of whether a two or a three engine plane is safer. The second p is a function of all sorts of mechanical factors that would only be known through a careful study of the design af an individual airplane type and is probably different for every single plane marketted. (The airframe and other critical systems are similarly more likely to fail on a plane that is running without its full complement of engines).

Engine failures are also not independent in another way. In a very recent crash, a pilot of a two engine plane got an indicator that one engine was on fire. He turned off an engine. Due to an unknown cause (pilot error, miswiring?) the wrong engine was turned off. On this flight two engines 'failed' even though one was in working order. From an engine designers standpoint, you might say that only one engine failed, but the plane still crashed. It could even be conceivable that a three engine plane after this occurence could get enough thrust from its remaining engine to allow a restart of the engine turned off in error.

But the survivability of a three engine plane in this case is not my point. The point is that engine failures are not necessarily independent events when talking about engines on a multiple engine plane.



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 8: Issue 18

# Monday 30 January 1989

# **Contents**

Hong Kong computer horse betting

George Moore

Kevcard badges vs. anti-shoplift systems

**Bruce Hamilton** 

Bank Fraud

Peter Golde

Crashing a PDP-11/40 (Computer Folklore)

Jeff Makey

Sprint to the Finish?

Steve Philipson

Information Security/Computer Crime Statistics

Stan Stahl

Re: ELIZA and Joe Weizenbaum

**Bernie Cosell** 

**Bob Krovetz** 

Virus conference hosts software swap meet

Robert Lee Wilson Jr

Structured Programs, Project Failures

Charles J. Wertz

Losing Systems

Mike Albaugh

Info on RISKS (comp.risks)

# Hong Kong computer horse betting

George Moore <georgem@microso.UUCP> Sun, 29 Jan 89 06:16:26 -0500

Tonight's "Beyond Tomorrow" program on Fox television did a short article about a device that is currently under test in Hong Kong. It is a portable (slightly larger than a calculator) terminal which allows a user to place bets on horse races from anywhere that has a modular phone connection. It has 6 touch-sensitive LCD windows which present various menus allowing the person to place up to 100 bets per race. Once all of the bets are entered, you just

connect it to the phone line and it dials up the computer at the race track. Your account number is stored in the (presumably) EEPROM of the device; all you have to enter is a 6 digit PIN number to identify yourself. Money won or lost is automatically reflected in your bank account.

The RISKS implications are enormous. People are currently grumbling on how unsecure an ATM is. That's nothing compared to this! At least with an ATM you have leased lines that are slightly harder to tap, with this wonderful device all someone has to do would be to tap a phone extension in your house or office and grab your PIN number. Even if it's encrypted, the thief will have plenty of time to break the code offline. After that he's free to deplete your bank account. With the proper fake ID, he could freely collect his winnings at the race track. Why gamble with your own money? Use someone else's!

The American Horse Racing Association is looking heavily into using this device in the U.S. to relieve overburdened telephone operators at most race tracks.

I for one, even if I \*did\* frequent the tracks, would never trust such a device over ordinary phone lines.

-George Moore

# Keycard badges vs. anti-shoplift systems

<"Bruce\_Hamilton.OsbuSouth"@Xerox.COM> 28 Jan 89 17:00:10 PST (Saturday)

Here's a new one. In Xerox/El Segundo we use these big heavy blue keycard badges that you slap against (or hold near) a reader to open various doors. Today I went shopping in the local Target store and as I tried to exit, all sorts of lights and bells went off. You guessed it -- the badge was responsible. The guard apologized and gave me a little piece of cardboard labeled "SCHLAGE SHIELD" to put next to my badge. Of course, when I got to work, I had to remove the cardboard to get the badge to work.

--Bruce

[Interesting. The same mechanism is used for entry control at Xerox and exit control (anti-theft) at Target. The moral unfortunately is that the SCHLAGE SHIELD works fine to circumvent the anti-theft control. Here is another supposedly high-tech solution with a trivial bypass. Ho-hum. PGN]

#### Bank Fraud

Peter Golde <ST501432@BROWNVM.BITNET> Sat, 28 Jan 89 22:47:49 EST

A few days ago I saw a program on TV dealing with bank fraud and mismanagement. One of the reports went somewhat as follows:

An employee in the computer division, who had been working at the bank less than a year, one day sent a computer message to the Brinks depository which stores and handles gold bullion for the bank. The message simply asked for Brinks to send 44 kilos of gold to such and such P.O. Box in a town in California. As per normal procedure, Brinks sent the money to the address, where the employee (or a confederate) picked it up. The employee then disappeared and still remains at large. Subsequent investigation revealed that the bank had never even checked his (phony) previous employment references when he was hired.

Boggles the mind, eh? One simple email message! --Peter Golde

# Crashing a PDP-11/40 (Computer Folklore)

Jeff Makey <Makey@LOGICON.ARPA>
30 Jan 1989 0132-PST (Monday)

In 1979 or so I heard a story that was already a couple of years old about a DEC PDP-11/40. It seems that one could walk across the room, kick the console terminal, and crash the computer.

After a certain amount of wailing and gnashing of teeth, they determined that walking across the room generated a static charge, which was transferred to the console terminal by kicking it. The (now dynamic) charge traveled down the communication wire to the terminal interface board and jumped across a narrow air gap to a neighboring circuit board, thereby disrupting things enough to crash the system. The problem was solved by moving one of the circuit boards to a different slot, which created too large an air gap for the charge to jump.

:: Jeff Makey

# Sprint to the Finish?

Steve Philipson <steve@aurora.arc.nasa.gov> Mon, 30 Jan 89 14:33:38 PST

In 8.16 a call went out for documentable stories on computer problems. I'm having one right now with US Sprint. Here's the story.

About a year and a half ago I moved from LA to the SF Bay area. I followed the instructions of my long distance carrier, US Sprint, which allowed me to keep my account while I moved, and to have it transferred to my new address when I established a new residence. A problem developed however, as Sprint set up a second account for me at my new address. I started to receive two bills each month, one for my calls placed from home, and another for those placed with the Sprint credit card. The two bills were for different account numbers.

I called Sprint about this, and they said they would consolidate the accounts, but I should send checks to pay the ammount due on each. I did so. Here lies the rub. Each time Sprint receives a check from me, they credit only account A. It makes no difference that I place the appropriate account numbers on both checks, and that they are sent in separately with billing forms for the appropriate accounts -- checks for account B get credited to account A. Sprint

now has submitted my account B to a debt collection agency. I have repeatedly called customer service and explained the problem, but they have taken no action, even though their records show two checks being credited to account A for each billing period. They have trouble believing that they could be screwing up their accounts receivables so badly.

I am now at the point of having my credit history being damaged by US Sprint, and may soon be contacting an attorney to sue them for same. Ah, the joys of dealing with a system where the "computer" makes no mistakes.

Note: If any readers out there work for Sprint, I'd appreciate your help in getting this problem fixed. Anyone know the name/address of the CEO?

# ✓ Information Security/Computer Crime Statistics

<Stahl@DOCKMASTER.ARPA> Sun, 22 Jan 89 22:57 EST

The National Center for Computer Crime Data is a non-profit organization devoted to the collection and dissemination of statistical information on computer crime, information security technology, and the information security profession. The Center is currently gathering statistics for its second report, "Commitment to Security." The Report is scheduled for release in May.

People with diverse backgrounds will read "Commitment to Security." These include information security professionals, including computer security practitioners, those in the R&D community, and sales and marketing personnel. Prosecutors and others responsible for enforcing computer crime laws will also read the Report. In addition, based on our experience with the first Report, the media will use "Commitment to Security" as a sourcebook on the extent and seriousness of computer crime. Consequently, it is important that the Report be as thorough, valid and meaningful as possible. Towards that end, we have surveyed 3500 computer security professionals and 2500 prosecutors.

There are, however, methodological questions about how best to measure and communicate the problems of computer crime and information security technology. Therefore, the Center would like to invite RISKS participants to engage in a conversation on these issues.

We would like to have a discussion in RISKS of questions like the following:

What statistics would enhance our understanding of the scope and seriousness of the computer crime problem?

What statistics would enhance our understanding of information security technology and its potential for reducing computer crime?

How can we best get valid statistics on computer crime and computer security technology?

How can we best present our information so that it is understood, both by the professional and the layman?

We will send a free copy of the report to anyone who meaningfully contributes to the discussion.

If you want to talk to us off-line, please call

```
JJ Buck BloomBecker, Director, NCCCD, 213/874-8233 or
```

Stan Stahl Research Director, NCCCD, 213/969-0777

Thanks, in advance, for your participation.

[By the way, Dockmaster has been off the net since just after this was posted. PGN]

# ✓ Re: ELIZA and Joe Weizenbaum

Bernie Cosell <cosell@WILMA.BBN.COM> Sat, 28 Jan 89 0:22:59 EST

```
} > Or, there's the story about the guy who falls asleep in front of his
} > terminal with an ELIZA program running and his boss logs on and thinks he's
} > talking to him but is actually talking to the program, and gets pissed off.
}
} This may have actually happened. Joseph Weizenbaum (MIT professor, author of
} _Computer Power and Human Reason_) told the anecdote in a class, with himself
} as one of the actors. It went something like this -- some of this is
} doubtless my own memory inventing things. The dialogue is partially courtesy
} of GNU Emacs' Eliza program, and the rest is made up.
}
} .... anecdote follows...
```

Is that for real, that Joe is telling that story? He has a lot of anecdotes, many of which appear in CP&HR, but I didn't know he was including one like that these days (alhtough such a thing must have SURELY happened some time or other at MIT). The REAL first round of that anecdote dates publicly to a small bit Danny Bobrow wrote in the first issue of some AI journal he started in something like 1968. The thing DID happen, although not quite as the word-of-mouth has transmitted it down to the present generation. The program in question was \_DOCTOR\_, \*\*NOT\*\* Eliza, and it happened at BBN, not at MIT.

I know all of this, because (Ta DAAH!) \*\*I\*\* wrote the original Doctor! Not \_Eliza\_ --- \_doctor\_: Weizenbaum's CACM article on Eliza had just appeared and for a variety of reasons I was looking for a neat Lisp hack to play with. The CACM article mostly told me enough, and I went off and wrote the thing. I can supply the details of the \*real\* "A Turing Test Passed" incident (the title of Danny Bobrow's article describing the event: it involved my version of doctor that I had left

running for people to play with to help me get it debugged, the "innocent third party" -- Danny Bobrow, and the Turing Testee, a random executive (whose name I will not reveal) who thought (for reasons that it is hard to figure out) that the Mod-33 was connected through to Danny at home early on a Saturday morning.

I can supply more details if anyone really cares, including (if I can dig the thing out of my archives) a copy of Bobrow's article about the incident which included the \*real\* typescript (danny came in later that Saturday morning and ripped it off of the terminal).

Bernie Cosell, BBN Sys & Tech, Cambridge, MA 02238

#### ELIZA and Joe Weizenbaum

<KROVETZ@cs.umass.EDU>
Mon, 30 Jan 89 02:26 EST

Bloom's story about Weizenbaum and ELIZA is close, but the person involved was Daniel Bobrow, not Weizenbaum. The account was described in the December 1968 issue of the SIGART Newsletter, and was reprinted in the book Machines Who Think, by Pamela McCorduck (p. 225).

The following is the description of the account:

"One Saturday morning about 9 A.M., a BBN Vice-President in charge of selling our Telcomp commercial service arrived at our PDP-1 computer room hoping to be able to use the computer for a demonstration. He found a note on the PDP-1 teletype that read: `TYPE ALL MESSAGES INTO THIS TELETYPE, AND END THEM WITH A PERIOD'. This note was left there by one of the programming bums who had just succeeded in making run a Lisp version of the DOCTOR program (based on ELIZA as developed by Weizenbaum). However, the VP thought that this note indicated that this teletype was linked with the one in my [Bobrow's] home, since I often used the computer all night. Therefore, he started typing to `me', but in fact was typing to this version of the DOCTOR program. The following conversation ensued:

VP: Do you think that I can use the computer this morning?

TELETYPE: Why do you ask?

VP: I might be able to make some additional telcomp sales.

TELETYPE: Why aren't you sure?

VP: My prospective customers have never seen a demonstration of the system.

TELETYPE: Does this mean very much to you?

VP: Of course it does.

TELETYPE: You seem very positive of that.

VP: This is ridiculous.

TELETYPE: What do you mean this is ridiculous?

VP: Is there any reason why I can't use the computer now?

TELETYPE: Tell me more about your prospective customers.

VP: Please dial me up on 491-1850

Note that after that remark the VP did not obey instructions and left out the period. Therefore, of course, the computer didn't answer him. This so infuriated the VP, who thought I was playing games with him, that he called me up, woke me from a deep sleep, and said:

VP: Why are you being so snotty with me?

BOBROW: What do you mean why am I being snotty to you?

The VP angrily read the dialog that 'we' had been having, and couldn't get any response but laughter from me. It took me a while to convince him it really was the computer".

Bob Krovetz krovetz@cs.umass.edu or krovetz@umass.bitnet

#### Virus conference hosts software swap meet

Robert Lee Wilson Jr <bobw@ford-wdl44>
Mon, 30 Jan 89 11:50:48 PST

I just received an ad from MIS Training Institure for "Micto/89 -- A Three-Day Conference on Microcomputer technology and its Impact on Security, Control, and Audit."

Among its concerns: "Indeed, with the recent front page coverage of the computer virus that struck universities, research, and government organizations across the country, one needn't be a security specialist to be aware of the problem."

So what is the first big benefit offered by the conference?

# " SPECIAL FEATURE Software Bonanza

o Software Swap

Bring diskettes with your original spreadsheet templates, BASIC, dBase, or other applications and swap them for the brainchild of a coregistrant. MIS will operate a Swap Center throughout the conference where we will maintain a library and make copies of diskettes for participants.

#### o Software Giveaway

When you attend the conference you will receive diskettes containing: Lotus 123 macros, utilities, virus detectors, graphics programs, and templates fot data analysis, statistics, investment analysis, and Lotus macros.

#### o Software Directory

Along with conference materials, you will receive an invaluable Directory listing over 1000 public domain and shareware programs you can obtain for little or no cost.

#### o MIS Electronic Resource Center

MIS' electronic bulletin board containing software programs, bibliographies, articles, audit programs, and much more will be available for your use during the Conference. "

The ad says the conference will "update you on new technologies and the risks to which they expose your organization." It sounds as if it might turn out to be a lab course.

**Bob Wilson** 

# Structured Programs, Project Failures

<<WERTZCJ@SNYBUFVA.BITNET> Charles J. Wertz Buffalo State College> Sat, 28 Jan 89 15:13 EDT

Over the last several months, there have been a number of articles touching on the above in Risks. Most of my computer career has involved the development of business systems for commercial enterprises. I never cease to be amazed by several things. And, I consider them to be contributing factors to the type of problem noted often noted here. They are -

- . the poor decisions which managers (both business and technical) often make for non technical reasons.
- . the haphazard approach many of our colleagues take toward requirements determination, requirement verification, and system testing.
- . the near crimes committed in the name of 'meeting the deadline".
- . the belief that following the externals of a methodology (such as indenting and naming rules or the format of a deliverable) is the same as understanding and following the methodology.
- the failure of many of our colleagues to understand or try to understand the reasoning processes behind the popular methodologies.

I'll resist the temptation to go on. I do believe that the above are primary explanations for many of the really poor business systems in existence today.

# ✓ Re: Losing Systems (RISKS-8.12)

Mike Albaugh <albaugh@dms.UUCP> Mon Jan 23 13:01:30 1989 > I would like to suggest that it would suffice anyway if it were applied. The > difficulty is that software is managed by programmers, not engineers.

Actually, both are, in my experience, managed by managers, who may not be either, but who owe their primary allegience to other managers.

- > Programmers have no tradition of quality of their own and insist that their
- > activity is so different from what engineers do, that engineers have nothing
- > to teach them.

I don't know what the first statement is suppose to mean, but it looks suspiciously like yet another of the gratuitous slaps that programmers typically get from engineers. For the record, I am officially a programmer, but have done a fair amount of hardware design (and been paid well by a satisfied employer for both). The major problem I have found is perhaps the name "software". Managers hear that and assume that changes to software are trivial (and free), while changes in hardware are impossible (or at least very costly.) The result, intended or not, is that programmers are required to add all sorts of software bandaids when the hardware fails to meet its spec. It is seldom actually acknowledged that this is happening, but the lack of acknowledgement does not mean a lack of happening. Especially in a project that involves custom LSI, there will be quite a few "enhancements" snuck into the software spec at the last minute (\_\_way\_\_ past "final" design review) that are nothing more or less than shoving hardware bug-fixes over the wall into the programmer's cubical.

> I am hopeful that the use of the term "case" presages the application of more > discipline in programming.

I could hope that some sort of documented "requirements control" would make these games more visible, but I doubt it will. They will, as usual, be swept under the rug as "clarification".

- > I also draw hope from the entreprenurial development of software for the > market, as opposed to works built for hire for a single organization. I saw
- > a great deal of quality software at Egghead on Saturday.

The great advantage an entrepeneurial firm has is that the president, Chief Engineer, and Chief Programmer have lunch together once in a while and can often get away with calling a spade a spade.

- > 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

Mike Albaugh (albaugh@dms.UUCP | | {...decwrl!turtlevax!}weitek!dms!albaugh)
Atari Games Corp (Arcade Games, no relation to the makers of the ST)
675 Sycamore Dr. Milpitas, CA 95035 voice: (408)434-1709
The opinions expressed are my own (Boy, are they ever)



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 8: Issue 19

# Wednesday 1 February 1989

# **Contents**

Massachusetts limits disclosure of driver's license database.

Jon Jacky

Dead Code Maintenance

**Douglas Jones** 

Re: Structured Programming

**Eric Roskos** 

Random Thoughts on Redundancy

**Earl Boebert** 

One last word about probabilities

**Dr Robert Frederking** 

Independence and probabilities

**PGN** 

Counting Engines

Mike Bell

Talk by Roy Saltman on computerized vote tallying **Charles Youman** 

Info on RISKS (comp.risks)

#### ✓ Massachusetts limits disclosure of driver's license database.

<jon@june.cs.washington.edu> Tue. 31 Jan 89 08:53:23 PST

This was sent to me by a friend who works at DEC. What I find notable about this story is the linkage between selling personal information in government databases to anyone who asks and legitimate law enforcement activities. It seems in this case it is felt you cannot limit the first without hampering the other. I can't tell from this account whether that is a technical consequence of the way the database works, follows from the legalities somehow, or is just a misconception.

- Jon Jacky, University of Washington

----- Forwarded Message

From THE BOSTON GLOBE, January 22, 1989, p.30

Registry Can Share Data With Police

The Massachusetts Registry of Motor Vehicles may continue to give computerize information to law enforcement agencies, at least until there is a final ruling on a privacy suit challenging that practice, the Massachusetts Appeals court has ruled.

The Appeals Court action modified an injunction issue last week by Superior Court Judge Joseph Mitchell. At issue is a challenge to a decades old Registry practice of which most holders of driver's licenses were not aware. For a small fee, the Registry has sold information about Massachusetts motorists, including Social Security numbers, to private businesses and anyone else who asked. The Registry - which has perhaps the largest computerized data base in the state - also routinely shares data with hundreds of law enforcement agencies and with registries in other states.

Citizens concerned about privacy filed suit against the Registry almost four years ago in Middlesex Superior court to block dissemination of their social security numbers and other personal data. Judge William Welch threw the case out on the grounds that the data collected and stored by the agency are "a public record." But in September, the Appeals court disagreed and gave the registry 60 days to show in Superior court why the information should not be kept confidential.

Last week, in Middlesex Superior Court Judge Mitchell issued a permanent injunction declaring the registry's information about a motorist's age, height or Social Security number "personal data" that may not be disclosed. The registry was banned from "distributing, offering, selling or making available" the data to anyone outside the registry. That ruling alarmed state officials who said it would cripple law enforcement efforts if the registry could not share information with police agencies.

The attorney general's office, representing the registry, warned that the agency would have no choice but to disconnect completely from the Criminal Justice Information System, which is connected to 500 Massachusetts and local police agencies. The system handles 125,000 requests a day for information - 25,000 involving Registry data.

"If the permanent injunction is not stayed, there would no effective enforcement of the motor vehicle laws within this state of any other state," testified Peter Larkowich, general counsel to the state agency that runs the information system. Without the data, he said, police could not identify motorists who cause or witness accidents and could not issue tickets "with any degree of certainty."

Robert Hernandez, the attorney representing the citizens in the

privacy suit, said his clients did not want to appear to be "cop killers", so they negotiated a partial stay of Mitchell's ruling.
"Basically, the feeling was that no judge was going to allow something to go on that would endanger the lives of law enforcement officers," Hernandez said. He said the registry would now have to warn motorists seeking a new license or renewing an old one that some of the information will be available to police. The registry will also have to inform motorists that they can request a randomly chosen number for their license number rather than their Social Security number.

The Appeals Court also said it would hear appeals from the citizens and the Registry on an expedited schedule.

#### Dead Code Maintenance

Douglas Jones <jones@herky.cs.uiowa.edu> Tue, 31 Jan 89 13:04:56 CST

One of the benefits I get from living in Iowa City is that many of my students have worked for one or the other of the local divisions of Rockwell International. One of them, who had worked for the Government Avionics Division, on the Global Positioning System project related the following tale to me:

Global Positioning System receivers are boxes that use information broadcast by a system of satelites to deduce the latitude, longitude, and altitude of the receiver. These boxes are built into a variety of weapons systems now in use by the United States and its allies. The box contains a radio receiver to listen to the satelites, and a fairly powerful computer to interpret the radio signals.

The computers in the current production GPS receivers are programmed in Jovial, although a new generation programmed in Ada will no doubt appear someday. My student was part of one of the teams that maintained the GPS code. After some time on the job, he began to realize that the code his team maintained was never executed and had never been executed in the memory of any team member. That is, an entire team of programmers was being paid to maintain dead code. Despite the fact that the code was dead, the team was required to produce the entire range of documents supporting each release of the code, and they were required to react to various engineering change requests.

Not too surprisingly, my student became demoralized and left the company, but not before learning enough to make the following hypothesis about how his situation had come to be.

He guesses that, once upon a time, there was a prototype GPS system where his module actually served some purpose and came to be executed from time to time. The structure of this system was presumably used to define Rockwell's contractual relationship to the Department of Defense, and as a result, his module gained a legal standing that was quite independent of its function in the GPS system.

As time passed, the actual calls to procedures in his module were eliminated from the GPS system, for one reason or another, until the code was dead. At first, nobody knew it was dead. The project was big enough that it wasn't uncommon for the people working on one module to have at best infrequent communication with those who called the procedures in the module, and engineering change notices that required changes to the module kept everybody busy.

Engineering change notices would not have arrived if the actual structure of the program were used to determine who needed to participate in a change. In fact, the notices were distributed based on many other criteria, including the contractual descriptions of the modules. The team was quite busy keeping their code up with the changes, testing changes using locally developed scaffolding, and waiting for any report of failures from the global system tests.

The discovery that the code was dead appears to have resulted from its passing global system tests even when it was obviously in error. Once my student found that the code was dead, he asked his managers why his efforts were being waisted on it. Their answer was that it was less expensive to maintain dead code than it was to rewrite the contract with the Department of Defense to eliminate the job.

Douglas W. Jones, Department of Computer Science, University of Iowa

# Re: Structured Programming

Eric Roskos <roskos@ida.org> Wed, 1 Feb 89 09:45:05 EST

- > What REALLY happens when a group of structured programmers tries to
- > develop a large program? Usually they argue about how the program should
- > be indented, what the comments should be like, how the subroutines
- > should be nested. ... etc.

If one believes that this is what "structured programming" is about, it is no wonder that there are such problems with it.

I wish I could give you some "war stories" about unstructured vs. programming, but unfortunately, all the software I've worked on has been proprietary, and I've only encountered a few insightful people who could tell from the outside which of the very large-selling software packages was internally well-structured, and which wasn't. Suffice to say that often there is a strong correlation between how easily a program can be adapted to meet new requirements and host system enhancements, and how well-structured the program is. Often it shows in the product architecture (how the features visible to the user interrelate) too.

There are at least two problems. First, "structured programming" seems to be one of those things you can learn only through experience; you discover it slowly through years of practice, during which time some the things that are taught as "structured programming" start to make some

sense, but only as a superficial veneer over what's really involved. Second, the sentiment expressed in the original article that "structured programming" is a bad thing in the development environment is widespread, and the disasters which result (which are very real to those who have had to maintain large programs) are often covered over by the developers, so that they are unknown on the outside. Sometimes a carefully-worded manual or an assortment of appealing new features can hide irreparable flaws in a program. Problems can result because, for instance, a programmer hardcoded a machine-specific feature throughout a several hundred thousand line program instead of isolating it in one place. Or because the code was made dependent throughout on the size of some data structure which was always referenced with a hard-coded constant offset rather than using some more "structured" reference. There are a lot of examples of this sort of problem, which has nothing to do with whether the program is "provably correct" or with how widely it sells. But it does have a significant bearing on how long the program will last without having to be rewritten.

Lately there seem to be new paradigms emerging (such as "object-oriented programming") which are intended to make some of these principles more obvious. They seem to have pros and cons, particularly in terms of efficiency, but perhaps the fact that there is so much programming to be done, and so few really experienced programmers out there, makes it necessary that some easier-to-understand concept take the place of "structured programming" for the most part. Just as there are not very many really well-designed products of any sort, there are not very many well-structured programs, and thus people tend to blame "structured programming" for what is, in reality, simply bad programming in a superficially neat and tidy style.

Eric Roskos, IDA (roskos@CS.IDA.ORG or Roskos@DOCKMASTER.ARPA)

#### Random Thoughts on Redundancy

<Boebert@DOCKMASTER.ARPA> Wed, 25 Jan 89 14:22 EST

From "Flight" magazine, many years ago: The Chairman of Rolls-Royce [which makes aircraft engines] was asked why he always flew the Atlantic in four-engined aircraft. His reply: "Because there are no five-engined aircraft." The same magazine once noted that a mechanical engineer looks out an aircraft window, sees four engines, and relaxes with a drink; the expert on fuel contamination looks at the same sight and tightens his or her seat belt. So maybe the only fundamental truth is that we are all prisoners of our metaphors, and never more so than in the software business.

On a less philosophical note, people interested in the issue of engine redundancy might find it worthwhile to look up the chapter in "Spirit of St. Louis" where Lindbergh presents the tradeoffs that led him to choose a single-engined aircraft for his attempt.

To get an idea of how such tradeoffs go, first consider my experience in working on the software design for a generic triple-redunant autopilot,

where I discovered that 85% of the logic was in redundancy management. This is a step forward in reliability?

Then look at the Honeywell autopilot for the Saab JA37b fighter. This was, as far as I have been able to tell, the first digital fly-by-wire system ever put in an operational aircraft. It was a single-channel system, with flight-critical functions backed up in the air data computer, and analyzed to a fare-thee-well (Honeywell had to \*demo\* that all possible short circuits between two arbitrary pins resulted in an orderly transition to the backup mode). Last I heard a couple of hundred of them had been flying for over a decade without incident. So redundant is neat, but simple and well-understood ain't bad either.

# One last word about probabilities

Dr Robert Frederking <ref@ztivax.siemens.com> Wed, 1 Feb 89 17:59:14 -0100

At great personal RISK to my ego, let me suggest that nobody has gotten the numbers right yet, even ignoring questions of whether independence, etc., holds in this case. For a three engine plane, where p is the probability of failure,

```
P(all three fail) = p**3
P(any 2 fail) = 3p**2(1-p)
P(any 1 fails) = 3p(1-p)**2
P(none fail) = (1-p)**3
```

This has the rather important property that all the probabilities add to 1. The key is to realize that the plane can be in eight states with respect to engine failure, each state's P is obtained by multiplication, and you add together all states that are essentially equivalent (differing only in which engine(s) are out). Thus

```
P(crashing) = 3p**2-2p**3, if it can fly on 2 engines.
```

```
Similarly for two engines,

P(both fail) = p**2

P(one fails) = 2p(1-p)

P(none fail) = (1-p)**2

which also happily adds to 1.

P(one or both out) = 2p-p**2, which (I believe) is always bigger.
```

As an aside, as I understand it, the FAA requires all airliners in the US to have more than one engine, and to be able to fly to a safe landing with one out.

```
Robert Frederking ARPA: ref%ztivax@siemens.siemens.com
Siemens AG/ZFE F2 INF 23 or : unido!ztivax!ref@uunet.UU.NET
Otto-Hahn-Ring 6 UUCP: ...!unido!ztivax!ref
D-8000 Munich 83 West Germany Phone: (-89) 636 47129
```

# Independence and probabilities

Peter Neumann <neumann@csl.sri.com> Wed, 1 Feb 1989 10:20:55 PST

It must be remembered throughout that the classical binomial probabilities assume independence. Cross-wiring throws that assumption for a loop. Subsequent to the 8 January crash of the British Midlands Airways 737 (where speculation still focuses on a wiring defect), FAA inspections have now turned up cross-wiring in engine or cargo-hold fire warning systems in at least four other planes. This is a particularly insidious type of problem, because it normally would be significant only in time of emergency, and under normal operation would have no effect (and remain undetected).

# Re: Counting engines

Mike Bell <mb@camcon.co.uk> 27 Jan 89 12:39:34 GMT

Of course, an increase in the number of aircraft engines actually \*increases\* the chance of catastrophic failure: if each engine has a probability p of losing a turbine blade in such a way that fuel lines are severed and a major fire ensues, then if an aircraft has N engines the probability of failure is clearly N\*p, so a one-engined jet is clearly safer, and a glider is safer still:-)

And then again, the complexity of systems interconnecting the engines increases non-linearly: you can't have cross-wiring faults between engines on a single-engined aircraft.

The point is simple: duplicating part of a system doesn't \*guarantee\* an improvement in overall safety, and indeed, can reduce it. ("This nuclear sub has two reactors so that if one should melt down, the second can...")

-- Mike Bell -- <mb@camcon.co.uk>, <mb@camcon.uucp> or even <...!ukc!camcon!mb>

# Talk by Roy Saltman on computerized vote tallying

Charles Youman (youman@mitre.org) <m14817@mitre.mitre.org> Wed, 01 Feb 89 11:14:38 EST

Roy G. Saltman of the National Institute of Standards and Technology (formerly NBS) will be speaking on the topic "Accuracy, Integrity, and Security in Computerized Vote Tallying" at the February meeting of the Washington, DC Chapter ACM. The meeting will be held on Thursday, February 16, 1989, at the Rosslyn Holiday Inn, 1850 North Fort Myer Drive, Arlington, Virginia. The talk will begin at 8:00 p.m. There is an optional dinner preceding the talk which starts at 7:00 p.m. Reservations are required only for the dinner (cost \$14) and can be made by calling (202) 659-2319 by noon on Tuesday, February 14.

The talk summarizes an extensive report on this subject recently published by Mr. Saltman at NIST. The talk concerns protections against manipulation

and fraud in the use of computer programs and hardware in computerized vote tallying. Recommendations concerning hardware, software, operational procedures, and internal control concepts are presented.

[Saltman's excellent report was cited in RISKS-7.52. 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 8: Issue 20

# Sunday 5 February 1989

# **Contents**

- FAA and flying under pressure in Alaska
- New use for Credit Cards (?) **Leslie Chalmers**
- Computer Chaos in Burnaby

Stuart Lynne

Swedish fighter plane crash

Otto J. Makela

Re: Massachusetts limits disclosure of driver's license database.

Jerome H Saltzer

"Computer Literacy Education" Report Available

Ronni Rosenberg

Engineering vs. Programming

Lynn R Grant

Re: Structured Programming

Al Arsenault

Allen Gordon

Dan Franklin

Info on RISKS (comp.risks)

# FAA and flying under pressure in Alaska

Peter G. Neumann < neumann@csl.sri.com> Fri, 3 Feb 1989 16:42:10 PST

Barometric pressure reached 31.85 inches at Northway, Alaska, on 1 Feb 89, the highest ever recorded in North America, and the third highest in the world. (This followed temperatures that unofficially reached -82 F; the official weather bureau thermometer conked out at -80.) Because most aircraft altimeters could not provide accurate readings, the FAA grounded all air traffic that would require requiring instrument approaches. [Source: San Francisco Chronicle, 2 Feb 89, p. A2]

### New use for Credit Cards (?)

<Chalmers@DOCKMASTER.ARPA>
Sat, 4 Feb 89 15:47 EST

The following appeared in a newsletter from my company's travel agency that came with an airline ticket I received recently.

The phrase 'one card does it all' is taking on new meaning. This month, Hyatt Hotels Corp. is testing a system that will allow a credit card to be used as a hotel room key. When the guest checks in by presenting a credit card, the hotel's system will alert its in-house system to allow entry to the guest's assigned room when the guest's credit card is inserted.

The new feature, to be tested at the Hyatt Regency in San Francisco, is just one element in the major hotel chains' efforts to increasingly cater to business travelers.

Automated check-in and check-out systems - with 800 numbers and videos - are already in place in some hotels. Watch for other chains to join the automation revolution. Ramada Hotels is evaluating a similar program that allows check-in, room key use and check-out all using a cellular machine. Guests will be able to slip the card through a machine for automatic check-in, and the machine will assign the guest a room and encode that room to accept the guest's card.

At check-out, a similar procedure is followed. When more than one guest is staying in a room, the hotel can make a blank card that will allow room entry.

I would say their are many risks associated with this (but not obvious enough for the hotels to notice), but the sentence that really stopped me was the last one. One interpretation of this is that the hotels will be equipped with credit card duplicating machines, some of which won't even be restricted to hotel employees! Granted, these duplicate cards won't \*look\* like real cards, but they will probably be good enough to fake out any machine which reads the mag stripe on cards. (Telephones which take credit cards come to mind immediately.)

An alternative interpretation is that the extra cards will be coded to contain values that are recognized by the hotel security system but which are not exact replications of the credit card mag stripe. I sure hope this is right, but somehow I doubt it.

Leslie

(The usual disclaimers apply.)

# Computer Chaos in Burnaby

pri=-10 Stuart Lynne <sl@van-bc.UUCP> 4 Feb 89 08:01:59 GMT

Yet another example of a very poorly executed computer system!

From the Vancouver Sun, Thursday, February 2, 1989 Burnaby's computer chaos started with obsolete system Jeff Lee - Sun Regional Affairs Reporter

A computer system Burnaby bought three years ago for \$200,000 that ended up costing more than \$1.2 million to make operational was obsolete when it was chosen, a report on the purchase indicates. The report released this week, also cited in-fighting among the muncipal departments, a flawed tendering process and lack of detailed plan as key reasons why the project "ran out of control."

Burnaby Mayor Bill Copeland said the report also shows council was not kept informed of the problems encountered in trying to make a prepared database system work effectively. "It was not flagged for council. Even though some of us (on council) were questioning the high cost of the system, at no time until it was too late did our staff come forward and say the had problems," he said. Copeland called the computer system "a money-eating monstrosity" and promised to find out why staff never told council, and why they never caught on to the fact the system was designed in 1965. He said it is too early to tell if staff will be disciplined, but council "is disappointed in our manager and director of administration. It appears our staff did not advise us when they should have.

#### Rumours circulated

Copeland said rumors had been circulating for some time about the systems's cost overruns, but no formal report was prepared until manager Mel Shelley ordered an independant audit in mid-1988. The report, prepared by consultant Brian Mullen, not only showed the system was obsolete, but said the decision to make "enhancements" to it to make it fit Burnaby's needs was unwise. The system failed an average of twice a week in 1988. It "is unreliable," Mullen said.

The municipality chose New York-based Information Associates Ltd. to provide the software after it received only two other bids, one of which was disqualified at an early stage. A staff report at the time said the system would cost \$118, plus an additional \$70,000 to modify the software to Burnaby's needs,. Mullen said many computer companies would have bid on the project had the system of tendering been relaxed. He said the terms of the bidding process were so retrictive that companies would have had to spend up to \$10,000 preparing for a \$100,000 bid. He also pointed the finger at infighting between the information services department and other agencies over the choice of the system. Nearly \$450,000 was spent on a computer consultancy firm that worked for 2 1/2 years trying to make the system work.

Municipal manager Shelley said he is preparing a report for council for Monday, and did not want to comment publicly before then. A spokesman for Information Associates' Canadian offices in Toronto could not be reached.

--- end of article ---

#### Comments:

- note politician trying to CYA by claiming that he wasn't informed.
- no overall plan

- over restrictive tendering policies limited competitive bidding
- office politics

Not noted in this article but mentioned in a smaller article last week was the fact that the requirements where changed frequently.

I'm going to try and track down some more info next week. But it seems that this is a clear case of incompentence on the part of the people in charge of the project. They don't seem to have handled \*anything\* correctly.

Stuart.Lynne@wimsey.bc.ca {ubc-cs,uunet}!van-bc!sl Vancouver,BC,604-937-7532

# Swedish fighter plane crash

<makela@tukki.jyu.fi> Fri, 3 Feb 89 13:18:49 +0200

The only existing prototype of the Swedish fighter plane JAS was destroyed in a crash at Linkoping on Thursday. The plane was making a landing after it's 7th test flight, when for reasons unknown the plane rolled sharply to it's left, causing the left wingtip to hit the ground. The plane then rolled wildly to the left side of the runway, losing it's wings and landing gear. Suprisingly enough, the main airframe was left relatively intact, and the pilot escaped with a broken arm.

According to specialists, the most probable cause of the accident was a technical failure. As the plane in question is designed for supersonic speeds, it is non-stable at subsonics. This would probably mean computer failure.

The whole accident happened before the cameras of the TV-Aktuellt crew. The fighter project has already been criticized severely, since is already 7 billion Swedish kronor (the American usage, ie 7000 million; around one billion US\$) over budget and 1 1/2 years late. The Saab-Scania military airplane section has contract for 30 JAS fighters at a fixed price, with an option for 150 planes more if there is an agreement on pricing. The Swedish air force has an estimated need for 300-400 planes after the year 2000. Also the Finnish air force has been interested in the plane.

Otto J. Makela (with poetic license to kill), University of Jyvaskyla

InterNet: makela@tukki.jyu.fi, BitNet: MAKELA\_OTTO\_@FINJYU.BITNET BBS: +358 41 211 562 (V.22bis/V.22/V.21, 24h/d), Phone: +358 41 613 847

Mail: Kauppakatu 1 B 18, SF-40100 Jyvaskyla, Finland, EUROPE

#### ★ Re: Massachusetts limits disclosure of driver's license database.

Jerome H Saltzer <jhs%computer-lab.cambridge.ac.uk@NSS.Cs.Ucl.AC.UK> Thu, 2 Feb 89 14:05:09 gmt

(RISKS-8.19)

[ From: <Saltzer@Athena.MIT.EDU> ]

Jon Jacky comments,

What I find notable about this story is the linkage between selling personal information in government databases to anyone who asks and legitimate law enforcement activities. It seems in this case it is felt you cannot limit the first without hampering the other. I can't tell from this account whether that is a technical consequence of the way the database works, follows from the legalities somehow, or is just a misconception.

The answer lies somewhere in between; it has little to do with computers or online databases, and civil libertarians in Massachusetts have fought a running battle on the subject for many years. The Registrar of Motor Vehicles has taken a position from time immemorial that your driver's license and your vehicle registration are matters of public record, and it has always made all the information in its files available to anyone who requests. With the automation of the Registry databases, the Registrar balanced the possibility of increased invasion of privacy against the possibility of increased revenue to the Registry (from selling the entire database on tape) and sprang for the revenue. Those of us who register their new car in Massachusetts are accustomed to receiving computer-generated letters from rustproofing companies that start out "Dear Mr. Smith: I'll bet you want to protect your investment in your new Toyota. . ."

Occasionally someone makes some progress against this particular problem; a few years ago the Registry grudgingly began to allow people to request that their social security number not be used as their driver's license identification number. But this flexibility is not publicized, and only those with enough interest in privacy to ask discover it. As a result you can construct a list of what some people would consider Massachusetts "troublemakers" by purchasing the Registry database and going through it to look for identification numbers that don't pass social security number validity tests.

The legal maneuvering that Jacky reported should be viewed in the light of the traditional Registry position. The first bid was to simply cut off all access to the information; I doubt that anyone expected that position to hold, but it had the entirely reasonable effect of forcing the Registry to make explicit arguments about who really needed to share the information and why. From a strategic point of view, the procedure may have been close to optimum--it took only two steps, and the result is certainly a big improvement. It remains to be seen whether or not the Registry finds some way to wriggle around the new rulings.

Jerry Saltzer

# "Computer Literacy Education" Report Available

Ronni Rosenberg <ronni@juicy-juice.lcs.mit.edu> Thu, 2 Feb 89 00:28:59 EST

Many thanks to all who sent me messages about computer literacy. In about three weeks, my Ph.D. thesis will be available as a technical report from MIT's Laboratory for Computer Science (LCS-TR-433, January 1989). If you would like a copy, you can request it from the lab or from me.

#### Engineering vs. Programming

Lynn R Grant <Grant@DOCKMASTER.ARPA> Wed, 1 Feb 89 16:00 EST

Over the years I have heard many arguments about why engineering is a science and programming is not, and I have even believed some of them, since I went to engineering school before I got into the computer business. It has finally occurred to me what the real difference is.

Engineers do a better job of design, not because they are more professional than programmers, but because they must. When you design a radio or an automobile, there are hundreds of people wo must get involved in order to build it. You can't sit down and discuss it with every one of them, so you must clearly document what you want in order to give them half a chance of building it right.

When you design a program, the design and the program can be one and the same, so a lower level of design documentation is possible.

As evidence of the fact that engineers design better because they must, not because they are by nature more professional, I submit the fact that microprocessors are being put into all sorts of formerly hardware driven devices, and hardware is being microprogrammed, for the most part, I believe, to get around the great overhead of engineering documentation. And we are now getting hardware that has the same sort of failures caused by insufficient design that we have always experienced in programming projects.

Lynn R. Grant, Consultant, Computer Associates International, Inc.

The opinions here are, of course, my own.

# Re: Structured Programming

Al Arsenault <AArsenault@DOCKMASTER.ARPA> Thu, 2 Feb 89 13:02 EST

I learned a couple of years ago that one can teach students some very valuable lessons about what 'structured programming' really is and why it's useful while they're at a relatively impressionable stage of their careers (I moonlight as an instructor of computer science at a local university.)

I noticed that many students had as an overriding goal getting the programs they write for class to work right - "style" and "structure" took a back seat to generating the right output. So, I assigned two projects, which were identical except that a particular data structure had to be implemented one way in the first assignment and a different way in the second one. Then, I gave the students approximately three weeks to complete the first assignment, but only about one week to do the second. (This was a second programming class for most students, and the assignment took about 1,000 lines of Pascal code, so it was a major undertaking for most student.)

The result was that those who had written the first program "properly" (i.e., lots of modularity, information hiding, and other buzzwords) had to make only a few modifications to complete the second assignment, while those who had programmed without any sense of structure got to write the entire thing over from scratch.

Several former students have since told me that it taught them a very valuable lesson, which they have carried with them into their professional careers.

It's something like spilling a drink on your keyboard: once you've been burned by something once, you usually learn not to do it again.

Al Arsenault

# ★ RE: Structured Programming (RISKS-8.19)

<GORDON\_A%CUBLDR%VAXF.COLORADO.EDU@CUNYVM.CUNY.EDU> Thu, 2 Feb 89 11:52 MST

I would like to add an example to the discussion of structured code etc. Several years ago I worked for a couple of years for a software house that produced a turn-key accounting system. It ran on a POINT 4 mini (DG NOVA clone) under IRIS. This is not a favorable environment for development! Worse the entire system consisting of over 1000 modules was written in Business Basic!. To make the matters worse the system was written for the Leasing Industry, which has perhaps one of most nightmarish accounting schemes imaginable since there are lots of ways to structure leases. Anyway, the design of the database was, in principle, masterful. There were master files which contained the names and locations of virtually every file, field and program, inaddition to the records and files which contained data. On the other hand the programs were written in a "spaghetti code", using 2-character variable names (the limit for business basic). No attempt was ever implemented to use some of the tools available and precompilers. Needless to say maintenance was literally a nightmare. Implementing changes were worse. If a field in a control or data file or record were changed, there was no way to track which of the 1000 modules were affected until after the modified software was put into use by the client and they screamed back at us.

The masterful design of the database was also one of its weaknesses. Everytime during data entry operations, a record was written to the database, a couple of hundred disk reads had to be performed in order to get all of the locations, etc., of the files, programs, etc. Since this was a time share system, multiplying that by 30 or 40 data entry operators in addition to other personnel doing various system operations, brought the system to its knees. The disk drives were simply overwhelmed with swapping and the necessary file read and write operations. Fixes were implemented but it was like installing after-market items on a '56 chevy to make it go fast. Of course even if the programs were structured, the performance problem would not have been fixed. The catch-22 was that because of the problems with maintenance we had no time to implement real fixes.

Allen Gordon

#### Re: Structured Programming

Dan Franklin <dan@WATSON.BBN.COM> Fri, 3 Feb 89 13:39:12 EST

A recent message on this topic asked if anyone was still carrying out studies of what programming practices contribute to errors. The answer is emphatically yes!

"Delocalized plans" are one example of a programming practice that's been demonstrated to cause errors. This phrase refers to a procedure for performing some action -- a "plan" -- whose steps are spread through the actual code -- "delocalized". Delocalized plans are a fruitful source of maintenance errors, because maintenance programmers generally don't (and often can't) read through an entire program before they start making what appears to be a small, localized change.

One recent article on delocalized plans appears in CACM, Vol 31 No 11 (November 1988): "Designing Documentation to Compensate for Delocalized Plans" (Soloway et al). The article is a bit more general than the title implies; the general problem of delocalized plans is discussed as well as documentation issues. (This article is a follow-on to discussions of delocalized plans in the book "Empirical Studies of Programmers", Soloway and Iyengar, Eds, Ablex, N.J., 1986, as well as an article in IEEE Software, May 1986, "Delocalized Plans and Program Comprehension".)

The authors discuss an experiment using a 14-module, 250-line Fortran program that performs simple database operations. Different programmers were asked to modify the program to add an "undelete" feature, which would restore deleted records in the database. It looks like a simple task, because deleted records are not actually removed, merely marked "deleted". The trick is that the obvious method of calling the search routine to find the record, then clearing the deletion mark, doesn't work because the search routine skips over deleted records. In other words, deletion itself is done by a "delocalized plan" that affects both the delete routine itself and the search routine. Many programmers asked to make the change didn't realize that.

This simple experiment shows a language-independent source of maintenance errors and (to me, at least) indicates that to the extent practical, you should try to group together all the steps that perform some operation, rather than scattering them throughout the code. Obvious? Perhaps; but in a world where some people think indenting code is a bad idea, even obvious conclusions apparently need to be demonstrated.

Dan Franklin



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 8: Issue 21

# Sunday 5 February 1989

#### **Contents**

<u>`User friendliness' tradeoffs can lead to total nonsecurity</u>

Eric S. Raymond

Capturing a password

Phil Karn

Collisions in DES

Jean-Jac. Quisquater

Re: Crashing a PDP-11/40 [static electricity]

Jeffrey Mogul

ATM error

**Douglas Jones** 

Anecdotes: ping-pong robot; CCC breaks net

**Konrad Neuwirth** 

Request for information: Health Hazards of Office Laser Printers

**Keith Dancey** 

Re: Structured Programming

Michael J. Chinni

Info on RISKS (comp.risks)

#### 'User friendliness' tradeoffs can lead to total nonsecurity

Eric S. Raymond <eric@snark.uu.net> 1 Feb 89 20:48:42 GMT

What would you say about a UNIX box vendor that included a section entitled 'How to crack into root privileges on this machine' in their manuals? Not much that's printable? Read on...

Yesterday morning my evaluation T5100 arrived from the good people at Toshiba America, their loan to my HyperNews project (it will be the field remote-test machine). I had great playing with this sleek little machine, assembling hardware and installing software and generally admiring the Neatness Of It All. Finally, a true portable capable enough to run a real operating system!

Installation was easy; the documentation took pains to make the system and

its setup procedures accessible to people who hadn't necessarily seen a UNIX before. Someone had obviously worked overtime on the `user friendliness' factor. I was impressed.

Between that and my own level of who-needs-the-manuals UNIX expertise it wasn't till this morning that I cracked the "T/PIX System Administrator's Guide", flipped through the Table of Contents and got a rude shock. There, staring up at me, was printed "Procedure 1.5: Forgotten Root Password Recovery"

"Ai yi yi!" I thought, and flipped hurriedly to the section. Sure 'nuf, it was a blow-by-blow description of how to do the boot-mount-and-edit trick every guru on a UNIX system with bootable floppies knows how to set up but seldom talks about -- and to make the trick easy the Toshiba people had helpfully supplied a microfloppy already built to do it with!

I wonder how much the Toshiba people thought about what they're doing. In their worthy concern with making it easier for novice administrators to recover from dumb errors without calling in an expert, they've broadcast a procedure that allows anyone who can get a copy of the tool disk and remember a few simple instructions to crack \*any\* T5100 they can get physical access to. And since these machines are portables it is unlikely they'll get much site protection.

If I needed one, this would have made a perfect and pointed reminder of the opposition between convenience and security, and the risks of designing for user-friendliness at all costs. As desktop and portable UNIX systems designed for serious and potentially sensitive work proliferate, I wonder how many vendors will make this kind of choice; how many others will leave that hole open though undocumented because "that's the way it's \*always\* been done"; and how many innocent users will become cracking victims for these reasons.

Eric S. Raymond (the mad mastermind of TMN-Netnews)

Email: eric@snark.uu.net CompuServe: [72037,2306]

Post: 22 S. Warren Avenue, Malvern, PA 19355 Phone: (215)-296-5718

# Capturing a password (Re: RISKS-8.18)

Phil Karn <karn@ka9q.bellcore.com> Thu, 2 Feb 89 00:22:09 EST

I once passed a REVERSE "Turing test". Back at Bell Labs in the early 1980s, we used a large PBX for terminal networking. Everyone had two phones on their desk: one for voice and another (with 212 modem) for data.

Late one night, my office-mate's data phone rang a few times and stopped. Thinking that someone had put the wrong number into their UUCP database, I set up a terminal and waited for the retry to see if I could spoof the UUCP login procedure and figure out the system responsible. Sure enough, a minute later the second call came. I typed "login: ". To my surprise, a human responded by typing her login name! "Hoookaaaay, let's try this," I muttered as I typed "Password: " The person obediently typed her password! After a few seconds I revealed who I was. Click. No more annoying calls.

Phil

#### Collisions in DES

Jean-Jac. Quisquater) < quisquat@prlb2.UUCP <jjq@prlb2.UUCP> 5 Feb 89 11:00:28 GMT

To avoid any incorrect rumor, here is the complete announcement:

We (Jean-Paul Delescaille and Jean-Jacques Quisquater) were able to find 3 collisions in DES using a network of workstations during some weeks.

Definition of a collision: given a message M and an cryptographic algorithm f with 2 parameters M and K (the key), a collision is a pair (K1, K2) such that

```
f(M, K1) = f(M, K2),
```

that is, for a fixed message M and using a cryptographic algorithm f, the key K1 and the key K2 give the SAME encrypted message.

Jean-Jacques devised a new probabilistic distributed asynchronous algorithm for finding collisions without any sorting and with a small storage (a la Pollard). We used a fast implementation of DES in C (by Jean-Paul: about 2000 \* (encryption + change of key) / second/machine)

We used the idle time of a network of 20 SUN-3's and 10 microVAXes (a la Lenstra and Manasse). Total: about 100 Mips during one month.

37

2 encryptions performed (about 20 potential collisions) only in software!

The message M is 0404040404040404 (hexadecimal form) for the 3 collisions.

Collision 1: found Fri Jan 13 23:15 GMT (birthday of Jean-Jacques! Yes, it is another birthday attack (Hi! Don Coppersmith)).

```
cipher = F02D67223CEAF91C

K1 = 4A5AA8D0BA30585A

K2 = suspense!
```

Collision 2: found Fri Jan 20 19:13 GMT

```
cipher = E20332821871EB8F
K1, K2 = suspense!
```

Collision 3; found Fri Feb 3 03:22 GMT

suspense!

Conclusion: Friday is a good day for finding collisions :-)

Well, there is a problem because there is no proof we effectively found such collisions.

Question 1: Find a protocol for proving or for convincing you that we know K2 for collision 1 (zero-knowledge protocols are useful in this context).

Question 2: Find a protocol for proving or convincing that we know K1 and K2 for collision 2 (idem).

Question 3: Find a protocol for proving or convincing that we know 3 different collisions (idem).

Useful information: the nice paper by Brassard, Chaum and Crepeau, "Minimum disclosure proofs of knowledge", 1987.

The complete information will be given at EUROCRYPT '89, Houthalen, Belgium, with the restriction that the submitted abstract is accepted:-) The paper will be sent in April if you want it.

Thanks are due to Paul Branquart, Frans Heymans, Michel Lacroix, Vincent Marlair, Marc Vauclair, the members of PRLB for permission and active help in the effective implementation of the distributed algorithm on their workstations.

Warning: There is no implication about the security of DES used for encryption. Indeed these experiments only prove that DES is a good random mapping (a necessary property for any cryptographic algorithm). However the use of DES for protecting the integrity of files is not very easy and needs very careful studies.

Jean-Jacques Quisquater (Program chairman of EUROCRYPT '89)

### Re: Crashing a PDP-11/40 [static electricity]

Jeffrey Mogul <mogul@decwrl.dec.com> 31 Jan 1989 1101-PST (Tuesday)

In <u>RISKS 8.18</u>, Jeff Makey writes about a PDP-11/40 that could be crashed by walking across the room and kicking the console terminal, thereby transferring a static charge to the console and the CPU.

I can confirm this feature of PDP-11/40s. When I was in high school, around 15 years ago, we had a PDP-11/40 (it's hard to believe that this machine, with 56Kbytes of RAM and a few Mbytes of disk, could serve 8 simultaneous users). I used to use the console occasionally, and found that when I was wearing a sweater knitted from acrylic wool I had to be careful not to let my arms rub on the case of the terminal.

We also had to go around the terminal room every few hours and spray some sort of anti-static mist over the ASR33s. I don't know if this really worked, or if we just had a placebo effect.

If a PC were this sensitive to static, typewriters would still be big sellers. It was extremely unpleasant to have to reboot every few hours on a dry winter's day. I still remember the sound made when I typed at a full-duplex ASR33 just after the computer stopped echoing.

-Jeff Mogul

#### ATM error

Douglas Jones <jones@herky.cs.uiowa.edu> Wed, 1 Feb 89 16:18:39 CST

I just had a run-in with an ATM that makes me wonder about the quality of programs (or is it programmers) used in the banking industry.

I went through the normal sequence, putting in my card, entering my PIN, and pressing the "FAST CASH, \$25" button.

It came back with the error message: "THE AMOUNT YOU REQUESTED IS NOT DIVISIBLE BY \$5.00." Then it gave me the option of entering a new amount or aborting the transaction.

I tried \$50.00, \$40.00, and \$5.00, and got the same result each time. I'd bet the machine was out of money, but if this is the case, the error message suggests incredibly ineptly written code.

Of course, a hardware error could add or drop a bit in a key storage location to make it think I'd asked for an odd amount, but such errors are rare enough that I wouldn't bet on it.

Oh yes, the ATM was relatively new, made by NCR, and at a very heavily used location.

Douglas W. Jones, University of Iowa.

# Anecdotes: ping-pong robot; CCC breaks net

Konrad Neuwirth <A4422DAE@AWIUNI11.BITNET> Sun, 05 Feb 89 18:34:19 MEZ

There is a nice(? find out for yourself) story about a Ping-Pong robot built at MIT. Now the guys who had built that machine were very proud of the device and wanted to show it to Mr. Minsky. First they explained to him how they built it, and made it recognize round objects with a certain amount of reflecting light, for what they had installed some lights, too. Now they turned on the lights, and started the software. One fact is important: mr. minsky is bald. They started the software, and he stand in front of the robot, directly in the lights..

\*\*\*\*T H A N G\*\*\*\*\*, and the robot hit the "ping pong ball".

The other one is about a German group of hackers (the CCC, Chaos Computer Club) breaking into a net. First about the net: it is called BTX (BildSchirmText = ScreenText) and is, well, sort of a mailbox system, but really more one way, as the lines are 1200/75 baud. Now there are

some banks taking part in the system, too. And there are pages, which yu have to pay for if you want to read them. Due to a security-leak, the CCC found out the password of one of the big banks in the system. They set up a page which you have to pay for, and made a computer (with the bank's account) dial up that page again and again and again......

They had the software running for a whole night, and in the morning, had 130.000 DM on their account.

But that's not all: they had warned the german Bundespost, who runs the BTX system, about the bug they had found in the system. The authities said "we have a bug-free system". And imagine, they also said that directly after the CCC had gone public with the hack! they said that the CCC must have had spies in the bank.

#### -konrad

p.s.: the bug was reproduceable. About the pong story: you can find it somewhere in Steven Levy's HACKERS book.

Konrad Neuwirth, Fernkorngasse 44/2/4, A-1100 Wien AUSTRIA Phone: +43 / 222 /604 15 30

### ★ Request for information: Health Hazards of Office Laser Printers

<kgd@informatics.rutherford.ac.uk>
Thu, 2 Feb 89 12:55:09 GMT

This is a request for information, or pointers to relevant sources of information, on the hazards of Laser Printers. I am more interested in the chemical health hazards than, say, heat and noise which are easy to appreciate. In particular, what is the wisdom of sharing office space without active ventilation with one or more Laser Printers?

I have a reference to arsenic compounds present on the drum, and a widely held "view" that the toner is carcinogenic, but nothing substantial and no authoritative source for the hazards these may pose.

I am also aware that erosion printers deposit light metals or other unpleasant material in the atmosphere, but then I am not familiar with this type of printer ever being used inside a permanently occupied office.

Perhaps the relatively recent development of desk-top laser printers pose a new hazard in those countries which do not habitually air-condition their offices?

Keith Dancey, UUCP: ..!mcvax!ukc!rlinf!kgd

Rutherford Appleton Laboratory, Chilton, Didcot, Oxon OX11 OQX

JANET: K.DANCEY@uk.ac.rl.inf

Tel: (0235) 21900 ext 6756

### Re: Structured Programming

"Michael J. Chinni, SMCAR-CCS-E" <mchinni@ARDEC.ARPA> Thu, 2 Feb 89 10:47:32 EST

One "war story" I can relate is the following. As an R&D computer facility we serve as what you might call a "job shop" for engineers at our site. One time an engineer came to us with a several thousand line program that he wanted us to put on our system (i.e. get it working). After accepting the job we found to our horror the the code was TOTALLY unstructured. It had NO comments; had no conection what-so-ever between variable names and their use; and frequently used system-specific code without mentioning that it was system-specific OR what the code did; and the entire program was replete with gotos.

It took us about 2 man-months of work to get that monstrosity working. However, if the code had been "structured" it would have taken us no more that 2 man-weeks.

The moral of the story is that had the code been structured we would have saved 1.5 man-months of work. And since we charge by time spent on a job, it would have saved much money.

Michael J. Chinni, US Army Armament Research, Development, and Engineering Center, Picatinny Arsenal, New Jersey



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 8: Issue 22

# Wednesday 8 February 1989

### **Contents**

B-1B bomber avionics problems

Jon Jacky

Risks of public terminal rooms

**Roy Smith** 

Using barcodes for road toll payments

**Phillip Herring** 

ATM error - in Europe

John O'Connor

Computing as a Discipline

Peter J. Denning

Cryptic status displays, and GIGO

Mark Brader

Re: `User friendliness' and forgotten root passwords

Shannon Nelson

Ge' Weijers

<u>smv</u>

Health Hazards of Office Laser Printers

**Hal Murray** 

Jeffrey Mogul

Re: Keycard badges vs. anti-shoplift systems

**Craig Leres** 

Info on RISKS (comp.risks)

### **✗** B-1B bomber avionics problems

jon@june.cs.washington.edu <Jonathan Jacky, University of Washington> Mon, 06 Feb 89 19:59:21 PST

Here are excerpts from AVIATION WEEK 130(1) Jan 2 1989 pps. 101, 103:

ROCKWELL WORKING WITH AIL TO DEVELOP B-1B AVIONICS FIX (no author)

Rockwell has more than two dozen engineers at AIL [an Eaton subsidiary] to work on the ALQ-161 which is designed to detect, indentify and jam enemy radars. ...

The problem occurs when an aircraft flies at low altitude over a powerful radar system. The system radar produces harmonics in the warning receiver that result in a large number of spurious signals overloading the ALQ-161 processor, which tries to analyze them as though they were actual threat emissions ... The fix essentially calls for screening out the spurious signals before they are digitized and allowed to enter the system processor ... Engineering work could be accomplished for about \$15 million. The modified system could be evaluated in a flight test by next fall or winter. The \$3.5 billion Air Force contract for development of the ALQ-161 was by far AIL's largest contract to date. The Air Force, meanwhile, has decided to study another approach to the problem which involves installation of an autonomous radar warning receiver in addition to the ALQ-161.

### risks of public terminal rooms

Roy Smith <roy@phri.phri.nyu.edu> Wed, 8 Feb 89 16:34:48 EST

Last week at USENIX, there was a public terminal room consisting of a bunch of terminals on an ethernet terminal server, and a Sun-3/60 with a dial-up SLIP line acting as an IP gateway to the rest of the world. People were invited to telnet to their home machines and read their mail (or whatever). It occured to me that if one was into such things, this would have been a golden opportunity to set up an ethernet listener to capture hostname/username/password triples. Given the high concentration of system administrators at USENIX, in the span of 5 days, one could have captured passwords for important accounts on most of the major Unix machines in the country.

### Using barcodes for road toll payments

Phillip Herring <ph@uowcsa.oz.au> Tue, 7 Feb 89 16:10:44 EDT

(From "The Australian"'s Computer section, Feb 7th, p. 55:)

"Barcodes, now in common use for identifying anything from cornflakes and library books to beer barrels, could also be the answer to speeding up the flow of traffic over Sydney's harbour bridge.

"Stickers carrying the barcode for the particular week or month could be sold at railway stations, lottery agencies or through the mail.

"These would be stuck to the side window of vehicles where they could be read by long-distance scanners at existing bridge checkpoints.[...]

"[A company representative] said the use of such technology on the bridge would enable vehicles to pass straight through if they were carrying the right barcode markings.

"If there were no sticker or the code was out of date, the normal default camera would be activated."

(From the second paragraph, it seems that everyone would get the same barcode for a given period. At \$1.50 (Aust.) per crossing, the new (manual) monthly passes will be worth a lot of money. With the Barcode system, anyone with a good printer and barcode-generating software would be in a good position to clean up with fake barcodes.)

Rev. Dr. Phil Herring,

University of Wollongong

# ATM error - in Europe

John O'Connor EuroKom < JOCONNOR@vms.eurokom.ie> Mon, 6 Feb 89 12:40 GMT

Recently when I was in Germany on holidays I used my Eurocheque card (once) to withdraw money from an ATM there - the ATM gave me no script of the transaction incidentally. It took about 3 weeks for the transaction to reach my account in Ireland. Fine - I saw it come in on the statement and marked it off against my records. Then 2 weeks later 2 more debits for the same amount came in. I checked my records before approaching my bank query the transaction. I was told that they would have to check back with the bank in Germany and examine its hardcopy audit of transactions etc. etc. and it could take 3 months for the amount to be refunded. The teller did however check with the international ATM office for the bank to discover that in the central clearing house in Brussels the German transaction tape had been mounted 3 times instead of once - causing chaos. The first erroneous transaction was corrected a few days later but it took more than a month to correct the second. My bank manager took a sympathetic view of my case and refunded the sum immediately, pending a correction from Brussels.

A few points in this case:

- 1. I find it unbelievable that this sort of error could happen in a major financial banking centre any other similar reports ?
- 2. My colleages said that they would not have spotted the error so quickly (or at all) too much trust in bank statements.
- 3. In the event of a dispute it was a case of my word against theirs I had no proof that I had NOT withdrawn the money.

John O'Connor, Systems Support, EuroKom, University College Dublin, Dublin 4, Ireland.

### Computing as a Discipline

Peter J. Denning <pjd@riacs.edu> Wed, 8 Feb 89 13:21:53 pst

A recent item in RISKS (Engineering vs. Programming, by Lynn R. Grant, in RISKS-8.20) about distinctions between engineering and programming prompts me

to invite RISKSers to read the report, "Computing as a Discipline," by the ACM Task Force on the Core of Computer Science. It is published in the January CACM and a condensed version on the February COMPUTER. It discusses these distinctions and more. The authors are Peter Denning (chairman), Doug Comer, David Gries, Michael Mulder, Allen Tucker, Joe Turner, and Paul Young.

### cryptic status displays, and GIGO

Mark Brader <msb@sq.sq.com> Tue, 7 Feb 89 18:57:01 EST

SoftQuad is one of the many companies that have decided lately that getting a FAX machine was a good idea. The one that we got supports delayed-start transmission to take advantage of overnight phone rates.

Last night, one of our managers left the machine set to send a document at 4:05 am to the 32nd phone number in the machine's memory, and went home.

And another employee came along, saw "D.XMT 0405#32" on the status display, decided this must be an error code, and helpfully removed the document from the feeder to try to clear the problem.

I asked the victim if it was okay to send this to Risks. He replied:

While you're at it you might comment on the highly confidential FAX I had to send some time ago. So confidential in fact that the recipient had to go to remove the FAX from the machine the moment it arrived so that no one would see it. Some time later, I got a puzzled call complaining that the FAX hadn't arrived.

I'd been so careful about making sure it was sent correctly, I'd put it in the machine wrong side down ...

Mark Brader, SoftQuad Inc., Toronto utzoo!sq!msb, msb@sq.com

### ★ Re: `User friendliness' and forgotten root passwords (RISKS-8.21)

Shannon Nelson <shannon@intelisc.intel.com> Tue, 7 Feb 89 00:19:11 pst

Don't be so shocked. That's taken directly out of the manuals from AT&T. My copy is the Prentice Hall publication \_UNIX(r)\_System\_V/386\_ \_System\_Administrator's\_Guide\_ for Systam V Release 3.0. Procedure 1.5 is indeed the procedure for "recovering" a forgotten root password. Actually, it's for replacing /etc/passwd with the original default file. The fact that you wipe out all of your account information is not mentioned. Also, the boot floppy that you are to use is meant for installing a new release, and automatically starts the process once UNIX is running. The procedure doesn't mention how to get out of that program and get a shell prompt. (Just hit the interrupt key at the first question)

Before attempting the procedure, I suggest making a copy of /etc/passwd.

# ★ Re: `User friendliness' and forgotten root passwords (RISKS-8.21)

Ge Weijers <ge@phoibos.cs.kun.nl> 7 Feb 89 09:36:34 GMT

There is no real protection against breaking into a system if you have physical access to it, IF it does not have any features that make booting from a random floppy impossible. Even without the boot disk it is quite easy to find the password file with a sector editor. One could boot the T5100 and run MS-DOS with the Norton Utilities or whatever to search for "root:" and change the password field to empty (making a hole in the 'gcos' field). Reboot Unix and type 'root'. No password check.

Who needs bootable Unix floppies? Some AT-clones have a feature which prevents bootstrapping from a floppy if switched on. A flag is stored in the clock chip. This 'feature' can easily be defeated by disconnecting the backup battery. (this is also true for BIOS-based password checks)

Systems containing sensitive data should not be physically accessible.

Ge' Weijers, KUN Nijmegen, the Netherlands
UUCP: ge@cs.kun.nl -or- uunet.uu.net!kunivv1.uucp!phoibos!ge

# Re: `User friendliness' tradeoffs can lead to total nonsecurity

<smv@apollo.com>
Tue, 7 Feb 89 18:31:32 EST

eric@snark.uu.net (Eric S. Raymond) writes in risks 8.21:

- > And since
- > these machines are portables it is unlikely they'll get much site protection.

I would expect a portable would be more closely attended than your average VAX. Most VAXen aren't at serious risk of being stolen while you get a cup of coffee. Also, most VAXen won't fit in an office safe, the Toshiba will. For the truly paranoid, there's always the large safe-deposit boxes at the bank, talk about secure computing! Even gets you mandatory signature checking at login. :-)

### ✓ Health Hazards of Office Laser Printers

Hal Murray <murray@src.dec.com> Mon, 6 Feb 89 22:43:43 PST

I used to work for Xerox, so I may be biased. I'm interested in that area, but not an expert.

You should be able to get that sort of info from the manfacturers. Your local

salesman may not be very helpful, but there is probably a corporate health or safety officer that worries about that sort of thing. He will probably be happy to send you copies of the reports that they have already filed with the government to certify that they meet all the rules. Try writing to the corporate headquarters.

I've seen the report sheet for the toner used in an LPS-40. It's not very interesting. If you can't get anything like it, I can probably send you a copy. I saw a similar one while I was at Xerox. It was equally dull.

Toner is almost inert. It's basically carbon black and ground up plastic. They stuff lots of it into rats trying to see if it does anything nasty.

I think the laser is powerful enough to be a problem if you look directly into it, but it is packaged inside a box ...

Yes, arsenic is an interesting chemical to use in a drum. I'm not sure what is acutally used these days. Things like arsnic are not usually very toxic until they get turned into a soluable compound. Copper and lead are toxic, but most people don't really worry about handling wire, pipe, or solder. (I've seen "wash your hands before eating" stickers on solder. I wonder if they teach that to plumbers?)

It's standard procedure to polish the drum, by hand, with a soft cloth, when tuning/cleaning a copier/printer. Next time I see a repairman, I'll ask. I don't remember that they were particularly careful with the cloth.

I did hear stories about early Xerox researchers working with selenium drums getting a strange body odor, but I don't remember any health complications that were part of the tale.

If I were looking for troubles, I'd try to find ozone. A dirty machine or such may make enough to be interesting. I can't remember the name, but there are thin high voltage wires used to charge the drum. Coronatron?

### Re: Health Hazards of Office Laser Printers

Jeffrey Mogul <mogul@decwrl.dec.com> 6 Feb 1989 1252-PST (Monday)

In <u>RISKS 8.21</u>, Keith Dancey asks about information on the hazards of office laser printers. I found a little information which might be useful. Digital (my employer) sells the LN03 printer, the guts of which are made by Ricoh. Included in the replacement toner cartridge kit is a "Material Safety Data Sheet"; I suspect that this information may be available from most other manufacturers.

The document lists, under "Hazardous Ingredients", two components of the toner: Ferrosoferric oxide 55%
Styrene acrylic resin 45%

The document goes into some detail on toxicity and first aid, but

the short summary would be that there are only "nuisance dust" problems.

The toxicity of each ingredient is also described:

Ferrosoferric oxide occurs in nature as the mineral "magnetite". No toxicity, other than that associated with nuisance dust is recognized.

Styrene Acrylic resin: This copolymer of styrene and acrylic acid has not been associated with a toxic effect in the open scientific literature, although the toxic effects of both styren and acrylic acid are well established. For practical purposes, the polymerization process apparently renders this substance biologically inert, only the nuisance dust properties associated with inhalation of large quantities of this material would be expected to be of biologic concern.

Nowhere in this document is carginogencity explicitly discussed, except to state that neither ingredient is listed in any of the following: Registry of Toxic effects of Chemical Substances (NIOSH), Occupational Safety and Health Administration, NIOSH, International Agency for Research on Cancer (WHO). I assume that this means that none of these organizations currently consider these ingredients toxic or carcinogenic, although that's purely an inference on my part.

Apparently, there are no "unusual fire or explosion hazards", no "hazardous decomposition products", and no "conditions to avoid".

"Other Precautions: Do not handle in areas where wind blows. Avoid inhalation of dust."

0 0 0

So far, so good, I thought. Then, I checked the Material Safety Data Sheet for Digital's LPS40 printer, also built on a Ricoh marking engine. This toner includes Styrene Acrylic Resin, but it also includes "dye" (nowhere else discussed) and Carbon Black. That rang a bell; sure enough, there is more question about this than the other toner.

Under "Toxic effects of ingredients":

### Carbon Black

Carbon black(s) have been tested for toxicity and carginogenicity in both animal exposure experiments and in epidemiologic investigations of exposed worker populations. Results of these investigations have been uniformly negative. Other than for the accumulation of carbon black in the pulmonary system, prolong exposure to carbon blacks produced no untoward effects. Benzene extractions of carbon blacks from some sources have elicited carcinogenic responses in animals, although the parent substance, itself, has been negative in this regard. The International Agency for Research on Cancer (IARC) has evaluated the evidence for the carcinogenicity of carbon black as inadequate to determine a carcinogenic risk for humans.

This document also states that "A review by the IARC of related polymers of [the two monomers used in styrene acrylic resin] was uniformally [sic]

negative."

For more information, I turned to "Dangerous Properties of Industrial Materials (6th ed)", by N. Irving Sax. About carbon black it says "Whiel it is true that the tiny particulates of carbon black contain some molecules of carcinogenic materials, the carcinogens are apparently held tightly and are not eluted by hot or cold water, gastric juices or blood plasma."

It is my recollection that newspaper ink contains carbon black; that might indicate the relative level of danger of carbon black in toner (although toner is inhalable, unlike printers' ink).

I don't normally add disclaimers to my messages, but I'm not speaking either as a representative of Digital or as an expert on this topic.

### Re: Keycard badges vs. anti-shoplift systems

Craig Leres <leres@helios.ee.lbl.gov> Tue, 07 Feb 89 00:44:49 PST

When I was in high school (about 10 years ago) they installed an inventory control system in our library. This spiffy new hi-tech system caught the immediate attention of a friend and me (who were sort of into lock hacking when we were in grammar school).

Obviously, we had to find out how the system worked and that meant stealing one of the widgets. Once accomplished, we disassembled it (it was made out of paper and foil) and then spent a few days theorizing about how the system worked. Luckly we had already studied electricity and magnetism in our physics class.

We were hard pressed to explain exactly how the widgets were detected by the exit sensors, but knew it had something to do with EMF or RF. I "borrowed" a small square of sheet metal from my metal shop class and, in a brave experiment, we demonstrated that a steel shield could be used to neutralize the widgets.

What we never figured out was why anyone would want a system that was so easily defeated.

Craig



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 8: Issue 23

# **Thursday 9 February 1989**

### **Contents**

Self-Taught Space Craft

**Brian Randell** 

Still a few bugs in the system, as they say

**Mark Brader** 

Multi-gigabuck information "theft"

Mark Brader

Risks of letting key people leave employment?

David A. Curry

Phone Risks

Greeny

Virus Technical Review

David J. Ferbrache

Re: WORM storage and archival records

**Curtis Abbott** 

Info on RISKS (comp.risks)

### Self-Taught Space Craft

Brian Randell <Brian.Randell@newcastle.ac.uk> Thu, 9 Feb 89 13:01:01 WET DST

SCIENTISTS TO BUILD SELF-TAUGHT SPACE CRAFT

By Mary Fagan, Technology Correspondent The Independent, 9 February 1989 (in its entirety)

Work by British scientists will enable future space craft to control themselves in flight without pilots, learning by trial and error in the way humans learn to walk or ride bicycles.

Technology being developed at the Turing Institute in Glasgow will allow satellites, space planes and space stations to learn to cope with the unexpected, including equipment failure and atmospheric changes.

Hotol, the British space plane which is involved in a long-running funding row, is to be at the heart of a one-year project to apply a form of artificial intelligence known as machine learning to flight control systems. This will allow Hotol to learn from its own experience, improving and adjusting flight performance as flight conditions change or things go wrong.

Although modern control theory for spacecraft is fine as long as nothing unpredicted happens, it cannot always cope with turbulence, if sensors fail or parts of the craft fall off.

Professor Donald Michie, of the Turing Institute, said: "The best analogy is a human riding a bike - if the handlebars fall off or something goes wrong, they can adjust their actions to regain balance. Balance is also very important for spacecraft and for satellites in orbit."

The work on Hotol, which will take off and land from airport runways, concentrates on machine learning for its initial ascent into space.

The concept, Professor Michie says, can also be applied to satellites subjected to unforeseeable fluctuations in solar winds and changes in air density. On large craft the huge solar panels could also be a source of instability.

The project is being launched by British Aerospace, which in spite of the Government's lack of support, has kept a large team on the Hotol project. The contract is the first signed under the Hotol Enabling Technology Club programme, which involves a group of companies which feel that software developed for Hotol could be valuable in other industrial areas.

Brian Randell, Computing Laboratory, University of Newcastle upon Tyne JANET = B.Randell@uk.ac.newcastle ARPA = B.Randell@newcastle.ac.uk PHONE = +44 91 222 7923

### Still a few bugs in the system, as they say

Mark Brader <msb@sq.sq.com> Wed, 8 Feb 89 18:00:06 EST

(Information from a Canadian Press wire service article carried in the Toronto Star, February 7. Wording is mine except for quotes.)

The Owner-Drivers Radio Taxi Service Ltd. of London, known as Dial-a-Cab, contracted to Mobile Data International Inc., of Richmond, B.C., Canada, for a computerized dispatching system at a cost of \$5.4 million (Canadian). Dial-a-Cab milked this for publicity and netted embarrassment. You guessed it. As Alf, one of their drivers, put it: "We'd made such a business saying we'd be the first in Europe to use this computerized system and it broke down within four hours."

And it's still sitting idle. Company chairman Ken Burns said: "It's not working ... A microchip has to be changed."

Another driver, Ben, said: "There was an overload. ... They hadn't fore-seen the amount of traffic on it." (That'd be 6,000 calls per day.) "We're blowing our tops about it. ... Everything was going to be action, action, action. But [it's] sitting in the cabs doing nothing."

Mobile Data's European sales director, Eric Dysthe, admitted the problems, but noted that Dial-a-Cab was "pushing for an early startup" before their annual general meeting. "That ... did not allow us to do the testing we should normally do."

Burns says Mobile Data says the problem is fixed but requires two more months for testing. The system has been installed in 1,450 cabs and the company, despite the problems, has ordered an additional 320 units.

Similar systems are widely used in Canada; the one in Toronto, which is reported to work well, is from a different supplier.

Mark Brader "Where is down special?" ... "Good."

Toronto "Do you refuse to answer my question?" "Don't know." utzoo!sq!msb, msb@sq.com

# multi-gigabuck information "theft"

Mark Brader <msb@sq.sq.com> <utzoo:msb@sq.UUCP> Wed, 8 Feb 89 17:41:08 EST

(Information from an article by Bob Mitchell in the Toronto Star, February 8. Wording is mine except for the quoted matter, which is from Constable Craig Lewers.)

A man has been arrested and charged with unauthorized use of computer information, following a 2-month police investigation. The suspect was an associate of a "very big" Toronto company: "a company that people would know ... with offices across Canada". Police are keeping the company's name secret at its request. They say the perpetrator acted alone.

A password belonging to the company was used to steal information which the company values at \$4 billion (Canadian): computer files belonging to an American company, believed [sic] to contain records from numerous companies, and used by large Canadian companies and the U.S. government.

"We don't know what this individual was planning to do with the information, but the potential is unbelievable. ... I'm not saying the individual intended to do this, but the program [sic] contained the kind of information that could be sold to other companies", said Lewers.

Mark Brader "Every new technology carries with it

SoftQuad Inc., Toronto an opportunity to invent a new crime" 
utzoo!sq!msb, msb@sq.com -- Laurence A. Urgenson

### Risks of letting key people leave employment?

<davy@riacs.edu>
Thu, 09 Feb 89 11:03:10 -0800

San Jose Mercury News, 2/8/89

TV editor charged in raid on rival's files

TAMPA, Fla. (AP) - A TV news editor hired away from his station by a competitor has been charged with unlawfully entering the computer system of his former employer to get confidential information about news stories.

Using knowledge of the system to bypass a security shield he helped create, Michael L. Shapiro examined and destroyed files relating to news stories at Tampa's WTVT, according to the charges filed Tuesday.

Telephone records seized during Shapiro's arrest in Clearwater shoed he made several calls last month to the computer line at WTVT, where he worked as assignment editor until joining competitor WTSP as an assistant news editor in October.

Shapiro, 33, was charged with 14 counts of computer-related crimes grouped into three second-degree felony categories: offenses against intellectual property, offenses against computer equipment and offesnes against computer users. He was released from jail on his own recognizance.

If convicted, he could be sentenced to up to 15 years in prison and fined \$10,000 for each second-degree felony count.

Bob Franklin, WTVT's interim news director, said the station's management discovered several computer files were missing last month, and Shapiro was called to provide help. Franklin said the former employee claimed not to know the cause of the problem.

At a news conference, Franklin said: "Subsequent investigation has revealed that, at least since early January, WTVT's newsroom computer system has been the subject of repeated actual and attempted `break-ins.' The computers contain highly confidential information concerning the station's current and future news stories."

The news director said Shapiro was one of two people who had responsibility for daily operation and maintenance of the computer system after it was installed about eight months ago. The other still works at WTVT.

Terry Cole, news director at WTSP, said Shapiro has been placed on leave of absence from his job.

Shapiro did not respond to messages asking for comment.

Franklin said Shapiro, employed by WTVT from February 1986 to September, 1988, left to advance his career.

"He was very good ay what he did," Franklin said. "He left on good terms."

### Phone Risks

GREENY <MISS026@ECNCDC.BITNET> Thu 09 Feb 1989 15:23 CDT

...Just when you thought the phones were safe, here is something to make you even more paranoid...

The other day I was on the phone with a collegue of mine discussing some things when he realized that he had to make a quick call to someone else. He placed me on "Consultation Hold" [where you can put the person you're talking to on hold, while calling another, and then go back to the first -- sorta like Call Waiting..]. Before he put me on hold, he said "If you're on hold too long then just hang up..."

Ten minutes later (I lost track of time typing something...), I was still on hold, when I was suddenly brought back to reality by a beeping in the phone. I figured that it was simply the phone system trying to signal him that I was still on hold and ignored it. After five minutes of this beeping, I gave up and hung up the phone. Then I left my office for a while.

About an hour later, my girlfriend came to my office and said "Gee you've been o the phone for a long time...". I hadn't so I decided to check and see if I might have left the phone off the hook, or if my modem had been automatically turned on by someone calling it up. Both turned out to be false, however, when I picked up the phone I was presented with BOTH SIDES OF A CONVERSATION THAT SOMEONE ELSE WAS HAVING. Clear as a bell, as if we were in a three-way call. So I tried to say something, but they couldn't hear me. Wierd I thought, must be a fluke, and hung up. Then I picked up the phone about 5 minutes later and they were still talking. 30 minutes later, this guy was talking to his girlfriend.

Enough was enough I decided, so I got on another extension and called the campus operator. She couldn't do anything of course, and recommended I call the Campus Features People. They also couldn't do anything, but said that they would leave a note for the network people in the morning. Just wonderful, I thought. And went home.

The next day, the phone was working, so I called the Telecommunications office on campus, and inquired as to what happened. The lady there said that she'd check it out and get back to me. About 10 minutes later she did and informed me that it was "a software problem in the switch" and to "call back immediately if it happens again". Oh great, I'm thinking. How can I ever be sure that my conversations are at least semi-private, and not screwed up all the time. This campus just recently had a multi-million dollar phone system installed (at least the first phase of it -- Audio), and I thought that it was relatively bug free. But recently strange things have been happening -- such as my phone playing "operator", and an ENTIRE dorm being cut off from phone service for about 6 hours.

...Yet another software bug....\*ho hum\* Does anyone out there know of a good, inexpensive, voice scrambler?

Greeny

### Virus Technical Review

"David.J.Ferbrache" <davidf@cs.hw.ac.uk> 9 Feb 89 10:53:21 GMT

This request has appeared on the bitnet virus-I mailing list, and has

been crossposted to the appropriate comp.sys groups and to comp.risks. I apologise for any readers who receive duplicate copies.

-----

A review of the threat posed to the security and integrity of microcomputer systems posed by self-replicating code segments

-----

I am in the process of compiling information on existing computer viruses, with a view to the production of a technical paper reviewing the threat to system security posed by both present computer viruses and likely future developments.

To this end I would be very grateful for information on individual infections, preferably detailing the symptoms observed, damage caused and disinfection techniques applied. Naturally I am also interested in details of the operation of the viruses, although I appreciate the reticence shown by infected parties to disseminate any details of virus operation, on the basis that it could lead to development of further viruses.

The technical report is part of a Doctoral research thesis in computer security, and will be available in late May. Distribution of the technical report will be restricted to people who have a legitimate interest (ie systems managers, commercial concerns, research), as I expect to review the techniques exploited by viruses in a fair degree of detail at the BIOS/DOS interface level. The report will consider the techniques used by virus to duplicate, the ways in which viruses gain control of the computer system, the camouflage techniques adopted and a brief overview of the existing computer viruses. Finally the report will consider the likely development of the threat from viruses, and how this developing threat can be addressed by protective software in both virtual and non-virtual machine operating environments.

At the moment I know of the following viruses:

### IBM PC MS/DOS

Lehigh variant 1 and 2
 New Zealand (stoned)
 Vienna (Austrian, 648)
 Blackjack (1701, 1704)

5. Italian (Ping Pong) 6. Israeli variant 1 (Friday 13th, 1813,

PLO, Jerusalem), variant 2, variant 3

(April 1st), variant 4

7. Brain (Pakastani) and variants 8. Yale

Also potentially variant of the Rush Hour and VirDem viruses developed during the CCC's work on viruses.

### APPLE MAC

1. NVir variant A and B, Hpat 2. Scores

3. INIT 29 4. ANTI

5. Peace (MacMag)

### APPLE II

1. Elk

**AMIGA** 

1. SCA 2. Byte Bandit

3. IRQ

ATARI ST

Boot sector
 Virus construction set viruses

Mainframe OS worms

1. Internet worm 2. DECNET worm

2. BITNET Xmas chain letter

I would be grateful for any information on these, or any other viruses. Reports of infection may be given in confidence, in which case they will only be used as an indication of geographical distribution of infection.

A summary of known viruses, their symptoms, geographic distribution and known disinfection measures will be posted to the list as soon as sufficient information is available to prepare an interim report.

As part of the paper I will also be reviewing the effectiveness of viral disinfection software, and would thus be interested in details of any software you use, its effectiveness, and availability.

Thanks for your time!

For those interested here is a summary of a few of the virus reports published on virus-I and usenet,

Subject, author and date Virus Virus-l issue

THE AMIGA VIRUS - Bill Koester (CATS) SCA LOG8805 comp.sys.amiga, 13 November 1987

New Year's Virus Report - George Robbins IRQ 1 January 1989, comp.sys.amiga

The Elk Cloner V2.0 - Phil Goetz ELK

26 Apr 1988

THE ATARI ST VIRUS - Chris Allen ATARI ST

22 March 1988, comp.sys.atari

Features of Blackjack Virus, Otto Stolz BLACKJACK v2.24

24 Jan 1989

Comments on the "(c) Brain" Virus BRAIN LOG8805

Joseph Sieczkowski, Apr 1988

Brain and the boot sequence, Dimitri Vulis BRAIN v2.5 5 Jan 1989

2 1911 1388

The Israeli viruses, Y.Radai ISRAELI LOG8805

2 May 1988

VIRUS WARNING: Lehigh virus version II LEHIGH v2 v2.35

Ken van Wyk, 3 Feb 1989

The Ping-Pong virus, Y.Radai ITALIAN v2.18

17 Jan 1989

Known PC Viruses in the UK and their effects MOST PC  $\,$  v2.23  $\,$ 

Alan Solomon, 1989

Yale Virus Info, Chris Bracy, YALE LOG8809a

2 Sep 1988

New Macintosh Virus, Robert Hammen ANTI

comp.sys.mac, 7 Feb 1989

Hpat virus-it is a slightly modified nVIR HPAT

Alexis Rosen, comp.sys.mac, 7 Jan 1989

INIT 29: a brief description, INIT 29 v2.18

Joel Levin, 18 Jan 1989

A detailed description of the INIT 29 virus INIT 29 v2.30

Thomas Bond, 27 Jan 1989

The Scores Virus, John Norstad SCORES LOG8804

info-mac digest, 23 Apr 1988

Macintosh infection at Seale-Hayne College TSUNAMI LOG8808d

Adrian Vranch, 8 July 1988

DEFENCE DATA NETWORK MANAGEMENT BULLETIN, DECNET (see also v1.59a)

50, 23 Dec 1988,

The internet worm program, an analysis INTERNET

Gene Spafford, Nov 1988

I apologise for any researchers whose articles I have not cited, in what is currently an incomplete list of references. Hopefully, this article will be of some use in providing a general list of viruses which have affected computer systems in the past.

Thanks for your time, and I look forward to any information you can supply me with.

Dave Ferbrache Personal mail to:

Dept of computer science Internet <davidf@cs.hw.ac.uk>
Heriot-Watt University Janet <davidf@uk.ac.hw.cs>
79 Grassmarket UUCP ...!mcvax!hwcs!davidf
Edinburgh,UK. EH1 2HJ Tel (UK) 31-225-6465 ext 553

# ★ Re: WORM storage and archival records

<abbott.pa@Xerox.COM> Wed, 18 Jan 89 15:43:23 PST

I think RAMontante <bobmon@iuvax.cs.indiana.edu>'s remarks deserve a response. Steve Phillipson's proposal of WORM devices for archival storage surely had to do with preventing electronic tampering. Physical tampering is quite another matter. Floppy disks and other electronic storage media are physical objects, and therefore subject to the same controls on authenticity and tampering as more traditional physical objects. Thus, a publisher of "authentic" Shakespeare could physically mark his disks in such a way that I can tell if the disk I get from RAMontante is authentic. Then what remains are problems like overwriting 0's with 1's (mentioned by PGN, I believe). There are lots of ways around this if you even believe it's a problem. (You might choose not to since only changing 0's to 1's already greatly limits the edits you can make.) For example, a single parity bit gives you a lot of protection (or rather, detection). Slightly more elaborate, and hardly more costly, schemes can give you full protection.

A perhaps relevant observation about the difference between paper and electronic media is that in the former, a certain degree of authenticity and tamperproofness is intrinsically bound up with the medium. It doesn't cost more, and you don't have to think about it. Those things aren't generally true of the newer media, so if we don't think about it, and pay for it, we sometimes get unpleasant surprises.

- Curtis Abbott



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 8: Issue 24

# Monday 13 February 1989

### **Contents**

- Massive counterfeit ATM card scheme foiled Rodney Hoffman **PGN**
- Computer blamed for 911 system crash Rodney Hoffman
- Risks of Selective Service **Rob Elkins**
- Re: Engines and probabilities **Barry Redmond** 
  - **Robert Frederking**
- Re: Structured programming Jim Frost
- Re: Engineering vs. Programming
  - John Dykstra
  - **Henry Spencer**
  - Robert English
  - **Shawn Stanley**
- Info on RISKS (comp.risks)

### Massive counterfeit ATM card scheme foiled

Rodney Hoffman < Hoffman. El Segundo @ Xerox.com > 12 Feb 89 14:25:22 PST (Sunday)

Summarized from a 'Los Angeles Times' (11 Feb 89) story by Douglas Frantz:

The U.S. Secret Service foiled a scheme to use more than 7,700 counterfeit ATM cards to obtain cash from Bank of America automated tellers. After a month-long investigation with an informant, five people were arrested and charged with violating federal fraud statutes.

"Seized in the raid were 1,884 completed counterfeit cards, 4,900 partially completed cards, and a machine to encode the cards with BofA account information, including highly secret personal identification numbers for

customers."

The alleged mastermind, Mark Koenig, is a computer programmer for Applied Communications, Inc. of Omaha, a subsidiary of USWest. He was temporarily working under contract for a subsidiary of GTE Corp., which handles the company's 286 ATMs at stores in California. Koenig had access to account information for cards used at the GTE ATMs. According to a taped conversation, Koenig said he had transferred the BofA account information to his home computer. He took only BofA information "to make it look like an inside job" at the bank. The encoding machine was from his office.

Koenig and confederates planned to spread out across the country over six days around the President's Day weekend, and withdraw cash. They were to wear disguises because some ATMs have hidden cameras. Three "test" cards had been used successfully, but only a small amount was taken in the tests, according to the Secret Service.

The prosecuting US attorney estimated that losses to the bank would have been between \$7 and \$14 million. BofA has sent letters to 7,000 customers explaining that they will receive new cards.

#### Massive counterfeit ATM card scheme foiled

Peter G. Neumann <neumann@csl.sri.com> Mon, 13 Feb 1989 13:33:12 PST

Note that, whether authorized or surreptitious, any access to the card information database -- IDs and PINs -- makes this kind of fraud rather easy. Unfortunately, the remedies are not easy. Even if the PINs were stored encrypted, a preencryption attack (offline) enumerating the 10\*\*6 possible PINs would compromise ALL of the PINs. Thus I conclude that the vulnerabilities here are considerable -- and grossly underestimated. (We have noted before in RISKS that the extent of credit card fraud is actually enormous, although the banks merely pass the losses on to the customers.) PGN

### Computer blamed for 911 system crash

Rodney Hoffman <Hoffman.ElSegundo@Xerox.com> 12 Feb 89 14:39:12 PST (Sunday)

Summarized from a 'Los Angeles Times' (12 Feb 89) story by Hector Tobar:

The Los Angeles city emergency 911 telephone system crashed twice Saturday afternoon. Pacific Bell said the shutdown was caused by "a power failure in the computer's signalling mechanism." For four hours, the system was only partly functioning as Pacific Bell engineers worked to repair computers at the dispatch center.

Operators first discovered the phone lines out about 1 pm. Pacific Bell engineers restored parts of the system 5 minutes later, but at 3 pm the system crashed again. A backup system also failed, stopping all emergency

calls for 45 minutes. Engineers once again restored the system's phone lines at 3:45. But the system's computers were still not working by late afternoon and the 25 operators at the dispatch center were forced to process calls manually. Computers normally display the address and phone number of the person making the call.

Operators at the center receive about 200 calls per hour. Callers who were unable to get through received a recorded message. Many then called police and fire stations directly. All calls were being answered by late Saturday. A police officer said it was fortunate that the breakdown occurred Saturday afternoon, during a quiet part of the weekend.

The computerized 911 system was installed in Los Angeles in 1983. Located four floors below ground level, it is designed to withstand a major earthquake. "It's a very good system," said a Pacifc Bell spokeswoman.

### Risks of Selective Service

Rob Elkins <relkins@vax1.acs.udel.edu> 10 Feb 89 17:20:42 GMT

Recently, a fellow student was sent a letter (computer generated of course) from the U.S. Selective Service System. The letter was a final warning to register in the selective service system before their name was submitted to the Justice Department for felony prosecution. What is ironic about all this is that this person is female and not required to register for Selective Service. Apparently, the computer system that they use maintains a list of female names and assumes that any individual whose name is not on this list must therefore be male. Her full name is Brantley Elizabeth Riley and when she called them to straighten the situation out, they told her that the system doesn't check middle names either.

Rob Elkins, University of Delaware

### Re: Engines and probabilities -- independence

"Barry Redmond, Lecturer, Telecoms Dept, KevinSt" <BREDMOND@dit.ie> Fri, 3 Feb 89 09:59 GMT

In RISKS-8.17 Craig Smilovitz writes:

>In the discussion about multi-engine aircraft failures, we've seen a lot of > mathematical probability exercises that forget about analyzing the basis > assumption about probability theory. That assumption is the \*independence\* > of the events in question.

Exactly.

There are many reasons why the probabilities are not independent. Just think about all the factors in common between the engines (2 or 3) on any single plane:

- -The engines are the same design
- -They were manufactured by the same company
- -They were fitted in the same factory
- -They were fueled from the same tanker
- -They were serviced by the same team
- ...and I'm sure you can all think of others.

If someone makes a mistake on one engine at any of these times, there is a high probability that they will make the same mistake on the other engine(s). The probabilities of failure are not independent because if one engine fails it immediately increases the probability of another failing.

In other words it's another manifestation of the old software debugging rule: "The more bugs you find, the more likely it is that there are more."

Barry Redmond, Dept of Electronics & Communications, Dublin Institute of Technology, Kevin St, Dublin 8 Ireland

### Re: Engines and Probabilities -- Good math, bad case analysis

"Robert Frederking" <ref@ztivax.siemens.com> 10 Feb 1989 08:33-MET

There was of course a mistake in my submission on the 2/3 engine controversy. While the P(one or both engines out) I gave was correct for two engines, this isn't the P(crashing), since it can fly on one engine. What I should have used was simply P(both engines out) =  $p^{**}2$ , which is indeed smaller than the P(2 or 3 out) for the three engine case.

Robert Frederking, Siemens AG/ZFE F2 INF 23,
Otto-Hahn-Ring 6, D-8000 Munich 83 West Germany Phone: (-89) 636 47129

### Re: Structured programming

Jim Frost <madd@bu-cs.BU.EDU> 12 Feb 89 16:56:02 GMT

It's possible that this topic has been overkilled, but I'd like to add several recent experiences to the "structured programming" argument.

My company markets a graphical database used for designing and testing event networks, which work much like PERT charts. Since the program is very graphical, it was written for the Silicon Graphics series of machines. Until recently, the SGI machines went for \$50,000 or more, somewhat limiting our market. I was hired to port the system to less expensive hardware.

On paper, the design of the system was very good. There were several major portions of code (graphics system, a thing like an interpreter, and a database). Unfortunately, the graphics system was written in a very unstructured format, using many global variables and splitting functions up in odd ways. Instead of being able to make small modifications to work on other

graphical systems, a complete rewrite had to be undertaken. After this rewrite, porting to new architectures has taken less than a week per architecture. The newer graphical systems are very, very structured.

Worse than the graphics, the other portions of the system were written by a programmer who must have had job security in mind. They are deliberately obtuse. Portions are very modular while others are so delocalized as to cause me to pound my head against the wall while trying to decipher them (why should a database manager make checks to see if the memory manager is still consistent?). We found that almost all of the modular portions ported with fair ease, while all of the delocalized portions had to be thrown out and rewritten.

What's the net result of giving proper structure to the product? The older system was so unreliable as to force our clients to run it under a debugger (gag). The newer is faster, easy to port, and much MUCH more reliable.

I'd say there's a lesson there.

jim frost, associative design technology

madd@bu-it.bu.edu

### ★ re: Engineering vs. Programming

John Dykstra - CDC Workstation Software < John D@CDCCENTR.BITNET> Thu, 9 Feb 89 13:43:16 CST

I've had the opportunity to be a logic designer on a high-end mainframe development project and an operating systems developer. There's one difference that leaps out at me: Hardware designers get to do the same thing more than once, while software designers, at least in the operating system area, always seem to be cutting new trails through the underbrush.

In these days of software-compatible product lines, it's not uncommon for the same hardware development team to implement an external architecture (the assembly language programmer's view of the machine) several times over the course of a decade. My company has two teams that are each on their third implementation, and you can see progressive improvements in the internal architecture (what the microprogrammer or customer engineer sees). Things get simpler, perform better and are more reliable. Of course, the constraints the team works under change (new LSI gate array technologies, requirements to support more multiprocessing, etc.), but hardware engineers get to learn from their mistakes.

The "building blocks" of hardware design also have not changed very much over time. We're still using registers, adders, control logic, microprogramming stores, etc. Techniques get extended over time, but I expect that you could show a 1950's digital engineer the logic prints for (say) an IBM 3090, and s/he'd be able to follow them easily. I don't think that someone who worked in AutoCoder back in 1960 would be able to read an Ada or LISP program, or even understand some of the basic concepts of the language.

Operating systems seem to take 5 to 10 years from beginning to maturity, so

most of us only do one or two in a career. Over a decade, requirements change enough that you can't just re-implement the previous system. For example, in the 60's batch processing was most important, while in the 70's you optimized for timesharing, and in the 80's distributed processing and networking are king. Hardware architectures also change, as support for virtual memory and hardware-support protection schemes is added, and of course we're using much different languages.

Basic design principles don't change, and sometimes they get codified into rulebooks such as "structured programming," and used by people who don't understand the "why" behind them. But the problems I'm trying to solve with my software design work are very different from the ones faced by the guy who occupied this office in 1979. Sometimes I'm thrilled by the challenge of finding my way through this wide-open universe of possible solutions, and sometimes I wish for the safety of designing yet another pipelined arithmetic unit.

I'll bet that the hardware designers on this list believe that they're in a tough situation, and that operating system design is easy! Does anyone want to make a case for that?

### ★ Re: Engineering vs. Programming

<attcan!utzoo!henry@uunet.UU.NET> Fri, 10 Feb 89 00:16:58 -0500

>When you design a program, the design and the program can be one and the >same, so a lower level of design documentation is possible.

On the one hand, this is certainly true. I heard the same thing from an EE friend of mine over a decade ago: he preferred software over hardware because changing the software was so much less hassle than updating drawings and such for hardware.

On the other hand, it is not obvious that this automatically means poorer quality. What we have here, actually, is a new version of the classical debate over whether word processing (or the typewriter!) leads to poorer writing. The more powerful tool definitely makes it easier to be sloppy, because less effort and thought is needed to get something out. But it also makes it easier to be perfectionist, because doing multiple iterations to get something absolutely \*right\* is much less hassle.

I think a fairer statement would be that the shift from hardware to software magnifies differences in how systematic and conscientious people are, and makes it harder for traditional hardware-oriented procedures (and older hardware-oriented managers) to catch the sloppy ones.

Henry Spencer at U of Toronto Zoology

#### uunet!attcan!utzoo!henry henry@zoo.toronto.edu

# Engineering vs. Programming

Robert English <renglish%hpda@hp-sde.sde.hp.com> Thu, 9 Feb 89 10:37:57 pst

The discussions about software system design have given many reasons for why those systems fail. It seems to me that those reasons can be broken into two main categories--technical and economic--and that any approach that attacks the first without somehow attacking the second as well is doomed to failure.

The immense complexity of software systems makes them difficult to build correctly. A large program can contain well over a hundred thousand lines of code, each of which would represent a moving part in a physical system. No one would expect a physical system that large and complicated to work reliably, at least not without extensive testing and redundancy.

But the technical problems go deeper than that. Physical systems are inherently modular. Each part has well-defined boundaries and performs well-defined tasks. While interactions between parts must be accounted for, these interactions are the exception, rather than the rule. Unless considerable care is taken, the opposite applies to software systems (even with modular software, the objects themselves tend to be more complex and less reliable than physical components).

Computer science has made great progress in addressing these technical issues. The need for documentation is well known, the benefits of proper coding practices have been well publicized, and the risks of buying or selling untested code have been demonstrated time after time. The economic problem remains unaddressed.

Physical systems take time to build. Every new part has to be designed and manufactured. Prototypes have to be built before they can be evaluated. It might take over a year to build a prototype for an automobile, and two or three years to set up an assembly line for a totally new model. Compared to such long product lead times, three or four months of testing are inconsequential. Developers are not, in general, the people doing the testing, so continued development is not seriously affected.

Software systems, on the other hand, take very little time to build. Each change makes its way into the system in the time it takes to recompile and reload. Thus, a software system that takes a year to build will have many times the complexity of a physical system taking the same amount of time, and the corresponding testing period should also be many times as long. In addition, effective software testing usually requires the same level of skill as software production, so that investment in testing adversely affects investment in future development. By greatly reducing the development time for a given function, software has greatly increased the relative cost of making that function reliable.

In a marketplace where time to market is the controlling factor in business

success, there is very little an individual programmer, system designer, or company can do to oppose these forces. A company that invests heavily in building reliable systems will lag far behind the market in other measures of system quality, such as functionality and performance, and will find itself limited to those niche markets where reliability is the overriding concern. Only if the marketplace changes so that those niche markets dominate will software reliability improve.

--bob--

# Re: Engineering vs. Programming

Shawn Stanley <shawn@pnet51.cts.com> Thu, 9 Feb 89 14:37:44 CST

There will probably always be a difference in opinions between engineers and programmers. Although they interact, they are not closely related fields, and thus have totally different problems.

For example, you can't take a test meter and check a program for discontinuity. And you generally don't heat-test a program for industrial use.

There are vast differences in debugging techniques, as well as design techniques.

UUCP: {uunet!rosevax, amdahl!bungia, chinet, killer}!orbit!pnet51!shawn

INET: shawn@pnet51.cts.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 8: Issue 25

# **Tuesday 14 February 1989**

# Contents

- Authenticity in digital media -- electronic time travel Steve Philipson
- Bogus Frequent Flver Scheme Kenneth R. Jongsma [and Dave Curry]
- Automatic targeting for Maverick missile Jon Jacky
- Economics, Engineering and Programming Jerry Leichter
- RE: ATM Error in Europe
- **Udo Voges** Another bank error Hsiu-Teh Hsieh
- Static Electricity crash

Seth K

- Legal clamp-down on Australian "hackers" **Neil Crellin**
- MIT virus paper available for anonymous ftp. Jon Rochlis
- Prospectus for "Computer Viruses" J Cordani
- Info on RISKS (comp.risks)

# Authenticity in digital media -- electronic time travel

Steve Philipson <steve@aurora.arc.nasa.gov> Tue, 14 Feb 89 10:18:50 PST

Two nights ago I saw a piece on Headline News that has some interesting implications. It seems Hank Williams Jr. found a previously unknown recording by his father, the late famed country singer Hank Williams, Sr. Hank Jr. decided that it would be great to make a new recording as a duet with his long departed Dad. From the news article, it sounded like the recording was heavily processed to remove noise and recording artifacts. In addition, film footage from a very old Kate Smith TV show was heavily

processed to show Hank Sr. singing this song (they implied that he did NOT perform it on that show), matching mouth movements to the lyrics in a very convincing manner. They also managed to merge an adult Hank Jr. into the scene as if he was there when it is was recorded. Quite a feat, as Hank Jr. was probably about 2 years old (or less) at the time.

The connection with RISKS is that computer/video processing technology has progressed to the point where seeing is definitely not believing. Not everyone is aware of this though, so the possibility exists that public opinion could be manipulated by showing influential people doing and/or saying things that are solely in the interest of the persons in control of this technology.

This is probably not new break-through in technology, but it is the first I've seen of it in national distribution.

Steve

### Bogus Frequent Flyer Scheme

<Kenneth\_R\_Jongsma@cup.portal.com>
Mon, 13-Feb-89 17:10:18 PST

Our local paper carried the following Associated Press story this evening:

An airline ticket agent piled up 1.7 million bonus air miles via computer without leaving the ground, then sold the credits for more than \$20,000, according to a published report.

Ralf Kwaschni, 28, was arrested Sunday when he arrived for work at Kennedy International Airport and was charged with computer tampering and grand larceny, authorities said.

Kwaschni, a ticket agent for Lufthansa Airlines, used to work for American Airlines, the Daily News reported today. Police said he used his computer access code to create 18 fake American Airline Advantage Accounts - racking up 1.7 million bonus air miles, according to the newspaper.

All 18 accounts, five in Kwaschni's name and 13 under fake ones, listed the same post office box, according to the newspaper.

Instead of exchanging the bonus miles for all the free travel, Kwaschni sold some of them for \$22,500 to brokers, who used the credits to get a couple of first class, round trip tickets from New York to Australia, two more between London and Bermuda and one between New York and Paris, the newspaper said. It is legal to sell personal bonus miles to brokers Port Authority Detective Charles Schmidt said.

Kwaschni would create accounts under common last names, the newspaper said. When a person with one of the names was aboard an American flight and did not have an Advantage account, the passengers name would be eliminated from the flight list and replaced with one from the fake accounts, the newspaper said.

"As the plane was pulling away from the gate, this guy was literally wiping out passengers," Schmidt said.

Just continues to show that the greatest security risk is the internal one.

Aside from the obvious mistake of using the same address for all his accounts, it would be difficult to catch this type of tampering. He was doing the type of operations that his job requires (adding and deleting passengers), so one wonders how American caught on.

Ken Jongsma

[Also noted by Dave Curry in the San Jose Mercury News.]

### Automatic targeting for Maverick missile

jon@june.cs.washington.edu <Jon Jacky, University of Washington> Tue, 14 Feb 89 10:10:14 PST

Excerpts from a story in FEDERAL COMPUTER WEEK, 13 Feb 1989, pages 29 and 37:

REDUCING PILOT BURDENS COMES UNDER RAPID FIRE, by Fred Reed

Automatic targeting continues its penetration of the military with the development of Rapid Fire, an automated fire-control system for the Maverick air-to-ground missile. The system, from Hughes Aircraft Co., is typical of approaches now being investigated by many manufacturers of several types of weapons . ... Maverick is a large anti-tank missile that homes in, by means of a sensor in its nose, on the infrared radiation emitted by tanks and other vehicles. ...

According to (Rapid Fire project manager Floyd) Smoller, the processing is possible with today's computers. Further, processing is less complex than in full-scale target recognition systems that seek to identify targets with certainty. ... ``The system does not give a hard and fast discrimination between tanks and other vehicles," Smoller said. ``However, it does favor tanks, based on variables such as size, aspect ratio and known signature. It rejects objects in its range that are too large to be vehicles --- roads, barns and so on. And it ignores fires so you don't shoot at burning tanks or forests."

Having found all candidate targets in its field of view, he said, the system chooses four targets, if the aircraft carries four missiles. "Then, if the pilot wants, he can simply fire at the targets or he can change the priority of the targets. The Air Force never likes to give up the final say on firing," Stoller said. ...

The two trends exemplified by Rapid Fire --- toward integration of computer, sensors, and weapons and toward increasing automation --- can be seen in many modern weapons. ... An Air Force spokesman said Rapid Fire seemed to be a good system but that the Air Force doesn't have a requirement for it now.

Hughes said it is working on an F-16 application to demonstrate Rapid Fire. The company believes the system will become more important as close air support grows in importance.'

### Economics, Engineering and Programming

LEICHTER-JERRY@CS.YALE.EDU <"Jerry Leichter> Tue, 14 Feb 89 12:41 EST

In a recent RISKS, Robert English points out that much of the pressure that leads to programs being shipped quickly, without extensive testing, is inherent in the economic structure of the industry.

He's very right. The following passage, forwarded to me by a friend, was taken from an article entitled "Technology and Competitiveness:" by John A. Young (who is president and CEO of the Hewlett-Packard Company):

"In today's world, shortening the time between idea stage and finished product often makes the difference between success and failure. The high costs of developing new products, the brief time before copies appear, and the rapid obsolencence make for a short innovation cycle-often 3 to 5 years (6). A study by the consulting firm McKinsey & Company demonstrated that for a typical product with a 5-year life span, a 6 month delay in shipping would reduce after-tax profits by one third. A 50% development cost overrun, by contrast, would reduce the after-tax profits by only 3.5% (13)."

### bibliography

- (6) F. Press, in A HIGH TECHNOLOGY GAP (Council on Foreign Relations, New York, 1987) pp. 14-15.
- (13) D. G. Reinertsen, WHODUNIT? THE SEARCH FOR THE NEW PRODUCT KILLERS (McKinsey & Company, New York, July 1983).

[taken from THE BENT of Tau Beta Pi - Winter 1989 issue]

Obviously, not everyone considers "6 month delay in shipping" and "50% development cost overrun" as the only two alternatives.

-- Jerry

### ★ RE: ATM Error in Europe (RISKS-8.22)

KFK/KARLSRUHE - Udo Voges <<IDT766@DKAKFK3.BITNET<> 02/10/89 09:16:11 CET

A similar error happened at the postal banking office in Munich: a wrong tape was mounted on 5 Jan 89 redoing all monthly transfers due at the end of the month. The error was discovered (due to customer complains?) and repaired the next working day (9 Jan) and apologies were mailed.

**Udo Voges** 

# Another bank error

Console Cowboy <vlsi005@ucscj.UCSC.EDU>

Sun, 12 Feb 89 02:02:44 -0800

This happened about a year ago in a small local bank which has been expanding its branches so far. One day I got a letter from a bank (computer generated one) informing me that my checking account has been closed. This was a shock to me, considering the fact that I have never requested my checking account to be closed. When I went to the bank to demand an explanation for the letter, the manager at the bank called up the central data processing facility in another location, and here is what she told me: my checking account was closed because it has not been accessed for 3 months, and since the balance was \$0.00. This was correct as far as I knew, but I have kept the balance in my checking account at \$0.00 for over a year then, since I have a share draft protection which means that whenever there is not an adequate fund in the checking account, adequate fund are automatically transferred from my savings account. So to simplify bookkeeping, I have kept my checking account on balance \$0.00 on purpose. Also, I had considerable fund in my savings account at the time.

Although the bank manager apologized for this error, I have changed to another bank since then.

Hsiu-Teh Hsieh, Univ. of Calif., Santa Cruz

### Static Electricity crash

<sethk@sco.UUCP>
Mon Feb 13 14:16:22 1989

Jeffrey Mogul (mogul@decwrl.dec.com) mentioned the following in <a href="mailto:RISKS-8.21">RISKS-8.21</a>:

- > In RISKS 8.18, Jeff Makey writes about a PDP-11/40 that could be
- > crashed by walking across the room and kicking the console terminal,
- > thereby transferring a static charge to the console and the CPU. (...)
- > If a PC were this sensitive to static, typewriters would still be big sellers.

Ever since SCO made the big conversion off of PDP-11/44's and on to PC's, we have been plagued by crashes due to static. While some machines seem more prone to this problem than others, it seems that any PC with a cartridge tape drive has the potential of crashing when the tape is inserted (and the correct conditions for static electricity exist). The policy recommended for those who handle backups here is to ground yourself to the chassis of the machine before/during insertion of the tape. I do not plan to sell my manual Olivetti typewriter yet.

-Seth (sethk@sco.COM)

### Legal clamp-down on Australian "hackers"

Neil Crellin <neilc@natmlab.dms.oz.au> Tue, 14 Feb 89 19:11:12 +1100

(Reproduced from The Financial Review, Feb 14th, 1989)

Clamp on computer hackers, by Julie Power

Federal Cabinet is expected to endorse today draft legislation containing tough penalties for hacking into Commonwealth computer systems. It is understood that the Attorney-General, Mr Lionel Bowen, will be proposing a range of tough new laws closely aligned with the recommendations of the Attorney-General's Department released in December. Mr Bowen requested the report by the Review of Commonwealth Criminal Law, chaired by Sir Harry Gibbs, as a matter of urgency because of the growing need to protect Commonwealth information and update the existing legislation.

Another consideration could be protection against unauthorised access of the tax file number, which will be stored on a number of Government databases.

If the report's recommendations are endorsed, hacking into Commonwealth computers will attract a \$48,000 fine and 10 years imprisonment. In addition, it would be an offence to destroy, erase, alter, interfere, obstruct and unlawfully add to or insert data in a Commonwealth computer system.

The legislation does not extend to private computer systems. However, the Attorney-General's Department recommended that it would be an offence to access information held in a private computer via a Telecom communication facility or another Commonwealth communication facility without due authority.

Neil Crellin, CSIRO Maths and Stats, Sydney, Australia. (neilc@natmlab.oz.au) PO Box 218, Lindfield, NSW 2070. (ph) +61 2 467 6721 (fax) +61 2 416 9317

### MIT virus paper available for anonymous ftp

Jon Rochlis <jon@ATHENA.MIT.EDU> Tue, 14 Feb 89 18:11:49 EST

The MIT paper on the Internet virus of last Novemember, "With Microscope and Tweezers: An Analysis of the Internet Virus of November 1988", is now available via anonymous ftp from either bitsy.mit.edu (18.72.0.3) or athena-dist.mit.edu (18.71.0.38) in the pub/virus directory as mit.PS (and mit.PS.Z). A version of this paper will be presented at the 1989 IEEE Symposium on Research in Security and Privacy.

-- Jon

### Abstract:

In early November 1988 the Internet, a collection of networks consisting of 60,000 host computers implementing the TCP/IP protocol suite, was attacked by a virus, a program which broke into computers on the network and which spread from one machine to another. This paper is a detailed analysis of the virus program itself, as well as the reactions of the besieged Internet community. We discuss the structure of the actual program, as well as the strategies the virus used to reproduce itself. We present the chronology of events as seen by our team at MIT, one of a handful of groups around the country working to take apart the virus, in an attempt to discover its

secrets and to learn the network's vulnerabilities.

We describe the lessons that this incident has taught the Internet community and topics for future consideration and resolution. A detailed routine by routine description of the virus program including the contents of its built in dictionary is provided.

# Prospectus for "Computer Viruses"

<"CORDANI, LTC J/A914-2469474" <cordani@pentagon-opti.army.mil<> 12 Feb 89 17:08:00 EDT

- 1. Dr. J Cordani, at Adelphi University, and E. Rustadt, at Pace University propose to bring out a collection of articles on the subject of computer viruses for the academic and research community.
- 2. We envision a volume of 10 to 20 articles, each 10 to 30 pages in length. We will attempt to cover the field of viruses in historical, social, ethical, economic, and technical areas.
- 3. We envision a section as introduction, theory, classifications, life cycles, epidemiology, countermeasures, economic and social issues, law, beneficial uses, the future.
- 4. As a member of this forum, I know of few more fruitful media in which to search for participants.
- 5. I should be most happy to discuss participation in the project with those interested.

Dr. John Cordani Schools of Business Adelphi University Garden City, NY 11530 (516) 663 1182

(My host system will be down from Feb 17 to Feb 24 from maint problems.)



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 8: Issue 26

# Wednesday 15 February 1989

## Contents

"\$15 Million Computer Dud Baffles Udall"

Joseph M. Beckman

Re: Computer blamed for 911 system crash

**Rodney Hoffman** 

Paul Blumstein

Selling who-called-the-800-number data **Bob Ayers** 

PIN? Who needs a PIN?

Alan Wexelblat

Door Sensors and Kids

Eddie Caplan

Risks of misunderstanding probability and statistics

Tom Blinn

Why you can't "flip" bits on a WORM disc

**Daniel Ford** 

Credit Checker & Nationwide SS# Locate

**David Andrew Segal** 

Re: Authenticity in digital media

Pete Schilling

Re: multi-gigabuck information "theft"

Jeff Makey

Info on RISKS (comp.risks)

## "\$15 Million Computer Dud Baffles Udall"

"Joseph M. Beckman" <Beckman@DOCKMASTER.ARPA> Wed, 15 Feb 89 16:45 EST

Summarized from the Washington Times (2-15-89): The US Office of Surface Mining has spent some \$15 million on a computer system to prevent strip mine law violators from obtaining new permits. The GAO is calling it a failure. The system apparently has a high error rate because it uses lists of names and addresses that are not complete. Arizonia democrat "Mo" Udall was quoted as saying "I'm really baffled. We have computer systems in this country to keep

track of everything from missiles to kindergarten kids who are sick or absent. But the Interior Department can't develop a system, even with the help of %15 million, to keep violators out of the coalfields."

By using the phrase "missiles to kindergarten kids" he seems to imply that systems are handling things as complex as missiles to as simple as... Of course, the fact that the subjects of the systems may be very complicated says nothing about what the system is actually doing.

Joseph

# Re: Computer blamed for 911 system crash -- more (RISKS-8.24)

Rodney Hoffman <Hoffman.ElSegundo@Xerox.com> 15 Feb 89 09:38:31 PST (Wednesday)

On Saturday, 11 Feb 89, the Los Angeles city emergency 911 telephone system crashed twice. The initial story, summarized in RISKS 8.24, blamed "a power failure in the computer's signalling mechanism." The `Los Angeles Times' (14 Feb 89) carried a follow-up story by Frederick M. Muir and Paul Feldman, with the following new information.

The crash was caused by one power converter board, an SL/1 positron switch, that helps control power fed to a complex switching system. It failed for still unknown reasons. It's an off-the-shelf part that involves a low degree of technology and sells for \$1000, according to Pacific Bell service manager Mike Fink. The switch recieves incoming 911 calls and routes them virtually instantaneously to the first open phone line.

"Fink said the board that failed is usually so reliable and simple that no backup was designed into the system. It is virtually the only part of the system -- which cost \$1.6 million to install -- without a backup."

Asked for past failure statistics, Pacific Bell and General Telephone, which between them operate hundreds of 911 systems across California, reported only two other failures in the past two years, neither of which was linked to the part which failed Saturday.

## Computer blamed for 911 system crash -- more (Re: RISKS-8.24)

paulb@ttidca.tti.com <Paul Blumstein> Wed, 15 Feb 89 09:29:23 PST

... The Los Angeles 911 system has had continual overload problems since its inception because it was expected that only 30-40% of emergency callers would use the system. The actual number turned out to be 75%. In addition, the system has received a large amount of non-emergency calls.

The overload has caused a several-minute delay during peak periods before a 911 operator could be reached.

Paul Blumstein, Citicorp/TTI, Santa Monica, CA

{philabs,csun,psivax}!ttidca!paulb or paulb@ttidca.TTI.COM

## Selling who-called-the-800-number data

Bob Ayers <ayers@src.dec.com> Mon, 13 Feb 89 12:59:53 PST

Those that liked the idea of states selling driver info will really love this one. As reported in the 20 February Forbes magazine, a new company, Strategic Information Inc ...

will collect, analyze and resell information on everything from retail prices in grocery stores to the premiums charged by insurance companies ... [it] intends to offer custom tailoring of such data to meet the needs of individual clients ...

One feature, available this spring through a 160-million-name database that Strategic recently purchased, will be marketed to companies with toll-free phone lines: For a fee, the companies can check the origins of any calls they receive through 800 numbers -- even those that don't go through -- enabling them to target the dialers for follow-up mailings or sales pitches.

### PIN? Who needs a PIN?

Alan Wexelblat <wex@radiant.csc.ti.com> Wed, 15 Feb 89 10:39:44 CST

Last night I had a rather frightening experience with my bankcard. Using one of the network of machines which is supposed to accept my card, I tried to make a withdrawal. The machine accepted my card, printed a message on its screen saying "Hello Alan Wexelblat, welcome to

#### Door Sensors and Kids

<eddie.caplan@H.GP.CS.CMU.EDU> Wed, 15 Feb 89 16:42:36 EST

While reading back issues of RISKS, I ran across the discussion here about automatic sensors for controlling doors. This made me recall that when we would bring our 2 year old son into work, he was not tall enough to trip the electronic eyes on the elevator doors. Subsequently, we always had to be sure to hold the door until he passed through or he would get bonked. The doors never closed hard enough to cause him any serious damage, but that's the RISK of the doors' hardware working properly.

# Risks of misunderstanding probability and statistics

Dr. Tom @MKO, CMG S/W Mktg, DTN 264-4865 <bli>solinn%dr.DEC@decwrl.dec.com> 15 Feb 89 08:37

As a person who has earned a doctorate in statistics, with emphasis on its practical applications (although I no longer work in that field), I have been both amused and appalled by some of the recent contributions focusing on probabilistic and statistical analysis of the risks of aircraft engine failures.

Some of the contributions assume, for example, that there really is such a thing as "the probability that one engine will fail", and that therefore you can compute the probability that two engines will fail (assuming that the failures are independent) by simply squaring this "p". This is such an incredibly simplistic way of looking at the problem that I'm amazed that anyone would offer it for consideration. Clearly, on any given aircraft, the engines share some subsystems in common; for example, they draw fuel from a common supply, possibly with a common fuel pump, possibly using two or more independent pumps. Certain failures in the common subsystems could cause both (or all) engines to fail. On the other hand, the engines have other subsystems that are not shared. While these unique subsystems may have been equivalent (and thus, have a common propensity to fail) at the time of manufacture, they almost certainly are not equivalent after any period of maintenance in the field. Consequently, even if we disregard the failures of common subsystems, the remaining engines almost certainly don't share a common probability of failure. Assuming they do can be an interesting and useful strategem for thinking about joint probability of failure, but it's a dangerous oversimplification.

In RISKS-FORUM Digest Volume 8: Issue 24, it is asserted by Barry Redmond that

>If someone makes a mistake on one engine at any of these times, there is a >high probability that they will make the same mistake on the other engine(s).

That may be true, but it may not be true, because the same person may not be working on all the engines. I would agree that an incompetent mechanic working on all the engines is likely to make the same mistakes on all of them, but the reality of aircraft engine repair is different.

>The probabilities of failure are not independent because if one engine fails it >immediately increases the probability of another failing.

This is a very interesting assertion. It seems to be saying that there is a causal relationship between a first engine failure and the likelihood of a second. Now, I would agree that if I were on an aircraft where one engine had just failed, I'd worry lots more that a second would fail as well then I usually would worry about engine failure when no engines had failed, but this doesn't mean that the probability of failure of the other engines has changed in any way. (It also doesn't mean that it hasn't, and if it has changed, it could be less or greater.)

It's unfortunate that a thorough grounding in probability theory and in statistical inference (and in risk analysis) isn't a part of the technical curriculum. Failures happen. They usually are not independent. Knowing how to analyse the risks of failures can help in making the tough decisions about where to put resources to "prevent" or "protect against" failures.

Tom

Dr. Thomas P. Blinn, Marketing Consultant, Application Platforms, U. S. Channels Sales, Digital Equipment Corporation, Continental Blvd. -- MKO2-2/F10 Merrimack, New Hampshire 03054

Opinions expressed herein are my own, and do not necessarily represent those of my employer or anyone else, living or dead, real or imagined.

# Why you can't "flip" bits on a WORM disc

Daniel Ford <daford@watdragon.waterloo.edu> Wed, 15 Feb 89 11:23:41 EST

Some contributors have noted that there are risks in trusting the integrity of data stored on indelible storage devices such as WORM type optical discs. These types of devices are often employed to store archival data that is never legitimately altered (bank records, school transcripts, transaction logs, etc.). There seem to be two risks to trusting this technology. The first is "How can you be sure that the disc you are reading is the original and not some altered copy?" and the second was "How can you be sure that some bits have not been 'flipped' by overwriting a disc sector with a new value that happens to burn a pit in the right spot?" The first concern is valid, but the second is not.

There are two reasons for this. Firstly, each disc sector on a WORM (and other types of optical discs) disc is protected with a sophisticated error correction code. These codes are very robust and are used because the very high storage densities of optical discs tend to give them correspondingly high error rates. So, if a bit (or several) was somehow "flipped", the ECC would either "correct" the change or report a read error.

The second reason has to do with how data is actually encoded on the disc surface. Contrary to what might first be thought, "pits" (the holes) and "lands" (space in a track between pits) do not correspond directly to 1's and 0's. Rather, their lengths and transitions form a sequence that encodes the data. Many codes have been developed, but a common one is NRZM (Non-return to zero mark). Basically, in this code the transitions between the lengths of both pits and lands record sequences of 0's and the transitions between the two record individual 1's. Certain minimum and maximum lengths of pits and lands must be respected for clocking and detection purposes.

In such a scheme, you cannot just flip one bit (by making a pit longer) you must flip two or more. So, even if you could get past the ECC, it would be quite difficult to get something specific and meaningful (i.e. not some weird control character in the middle of someone's name) by overwriting a WORM disc sector.

Further, each sector overwrite will also overwrite the ECC and change its encoded value, which is burned into the disc along with the data, to some other value. As such, it is unlikely that the ECC and the sector contents will remain consistent after an overwrite (giving subsequent read errors).

It would be much easier to forge a disc and substitute it for the real thing then try to alter the original. But, safeguards against that can be developed as well.

Dan Ford

[Thanks for the elaboration. But remember that even if you have an N-error detecting code, many (N+1)-bit falsifications will go undetected. Similar problems exist with ECC. PGN]

#### Credit Checker & Nationwide SS# Locate

David Andrew Segal <dasegal@brokaw.LCS.MIT.EDU> Wed, 15 Feb 89 16:52:28 EST

A member of my research group received the following "comforting" advertisement in the mail (comments in [] are my editorial remarks...):

CREDIT CHECKER & NATIONWIDE SS#-LOCATE just got
BETTER!

PROFESSIONAL CREDIT CHECKER has always offered:

- \* Consumer Credit Reports from thousands of credit sources coast-to-coast.
- \* Social Security Number tracing anywhere in the country.
- \* Driver's License reports from every state but Massachusetts [See Risks 8.20]
- \* Financial reports on over 9,000,000 businesses all across the USA.

and now,
PROFESSIONAL CREDIT CHECKER
offers an exciting NEW service: [oh, boy]

NATIONAL ADDRESS/IDENTIFIER UPDATE!

With NATIONAL ADDRESS/IDENTIFIER UPDATE you can enter either a name and address or a Social Security Number. The Network will search all over the nation and get a complete report back to you in just seconds!

You can get such information as all current names, aliases, social security numbers and/or variances, date of birth, present and past employers and past and/or present addresses.

You can find people anywhere in the country without having to access a full Credit Report. No permissible purpose under the Federal Law is required to run NATIONAL ADDRESS?IDENTIFIER UPDATE...and NO RECORD of an inquiry will be logged on the consumer's credit report! ... [Boy, it isn't illegal and no one will ever no you invaded their privacy!]

----END OF ADVERTISEMENT-----

I think the ad says it all.

David Andrew Segal, MIT Laboratory for Computer Science

[And don't forget the on-line National Credit Information Network mentioned in RISKS-8.11. PGN]

# Re: Authenticity in digital media (RISKS-8.25)

"ALBTSB::SCHILLING1" <schilling1%albtsb.decnet@aldncf.alcoa.com> 15 Feb 89 14:51:00 EST

Seeing hasn't been believing for a long time. Remember Fred Astaire dancing on the ceiling in the movie "Singing in the Rain"? And the newsreel footage showing Hitler dancing a little jig in front of the Eiffel Tower after the French surrender in WWII was a good piece of 1940 film editing, not an accurate motion picture. Counterfeit paintings in the style of well-known artists have been around for at least four hundred years. The Shroud of Turin was recently found to date from the 13th instead of the 1st century A.D. Counterfeit coins were a problem in Roman Empire.

Computers haven't cut us off from history. They just provide new tools with which human beings can fool one another.

Pete Schilling, Alcoa Laboratories

## Re: multi-gigabuck information "theft"

Jeff Makey <Makey@LOGICON.ARPA> 14 Feb 1989 2127-PST (Tuesday)

In <u>RISKS DIGEST 8.23</u> Mark Brader <msb@sq.sq.com> paraphrases a recent article from the Toronto Star:

>A password belonging to [a large Canadian] company was used to steal >information which the company values at \$4 billion (Canadian) ...

This report isn't news. The "computer files" are nothing more than the source code for AT&T's UNIX operating system, copies of which may be easily obtained for a license fee on the order of a few thousand dollars -- a far cry from \$4 billion. I suspect that AT&T's lawyers are at the root of this sensationalism.

Jeff Makey



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 8: Issue 27

# Thursday 16 February 1989

# Contents

- FBI NCIC Data Bank
  - **Bob Morris**
- Internet mail forgery
  - Walter Roberson
- Re: Dead code maintenance
  - **Clifford Johnson**
- Probabilities and Engines
  - Steve Philipson
  - **Robert Dorsett**
  - Daniel A. Graifer
- Info on RISKS (comp.risks)

## FBI NCIC Data Bank

<RMorris@DOCKMASTER.ARPA> Thu, 16 Feb 89 09:41 EST

Proposed FBI Crime Computer System Raises Questions on Accuracy, Privacy --Report Warns of Potential Risk Data Bank Poses to Civil Liberties Washington Post, February 13, 1989 by Evelyn Richards

On a Saturday afternoon just before Christmas last year, U.S. Customs officials at Los Angeles International Airport scored a "hit."

Running the typical computer checks of passengers debarking a Trans World Airlines flight from London, they discovered Richard Lawrence Sklar, a fugitive wanted for his part in an Arizona real estate scam.

As their guidelines require, Customs confirmed all the particulars about Sklar with officials in Arizona - his birth date, height, weight, eye and hair color matched those of the wanted man.

Sklar's capture exemplified perfectly the power of computerized crime fighting. Authorities thousands of miles away from a crime scene can almost instantly identify and nab a wanted person.

There was only one problem with the Sklar case: He was the wrong man. The

58-year old passenger - who spent the next two days being strip-searched, herded from one holding pen to another and handcuffed to gang members and other violent offenders - was a political science professor at the University of California at Los Angeles.

After being fingered three times in the past dozen years for the financial trickeries of an impostor, Sklar is demanding that the FBI, whose computer scored the latest hit, set its electronic records straight. "Until this person is caught, I am likely to be victimized by another warrant," Sklar said.

Nowhere are the benefits and drawbacks of computerization more apparent than at the FBI, which is concluding a six-year study on how to improve its National Crime Information Center, a vast computer network that already links 64,000 law enforcement agencies with data banks of 19 million crime-related records.

Although top FBI officials have not signed off on the proposal, the current version would let authorities transmit more detailed information and draw on a vastly expanded array of criminal records. It would enable, for example, storage and electronic transmission of fingerprints, photos, tattoos and other physical attributes that might prevent a mistaken arrest. Though controversial, FBI officials have recommended that it include a data bank containing names of suspects who have not been charged with a crime.

The proposed system, however, already has enraged computer scientists and privacy experts who warn in a report to be released today that the system would pose a "potentially serious risk to privacy and civil liberties." The report, prepared for the House subcommittee on civil and constitutional rights, also contends that the proposed \$40 million overhaul would not correct accuracy problems or assure that records are secure.

Mostly because of such criticism, the FBI's revamped proposal for a new system, known as the NCIC 2000 plan, is a skeleton of the capabilities first suggested by law enforcement officials. Many of their ideas have been pared back, either for reasons of practicality or privacy.

"Technical possibility should not be the same thing as permissible policy," said Marc Rotenberg, an editor of the report and Washington liaison for Computer Professionals for Social Responsibility, a California organization. The need to make that tradeoff - to weigh the benefits of technological advances against the less obvious drawbacks - is becoming more apparent as nationwide computer links become the blood vessels of a high-tech society.

Keeping technology under control requires users to double-check the accuracy of the stored data and sometimes resort told-fashioned paper records or face-to-face contact for confirmation. Errors have plagued the NCIC for many years, but an extensive effort to improve record-keeping has significantly reduced the problem, the FBI said.

Tapped by federal, state and local agencies, the existing FBI system juggles about 10 inquiries a second from people seeking records on wanted persons, stolen vehicles and property, and criminal histories, among other things. Using the current system, for example, a police officer making a traffic stop can fine out within seconds whether the individual is wanted anywhere else in the United States, or an investigator culling through a list of suspects can peruse past records.

At one point, the FBI computer of the future was envisioned as having links to a raft of other data bases, including credit records and those kept by the Immigration and Naturalization Service, the Internal Revenue Service, the Social Security Administration and the Securities and Exchange Commission.

One by one, review panels have scaled back that plan."

"There's a lot of sensitive information in those data bases," said Lt.

Stanley Michaleski, head of records for the Montgomery County [Maryland]

police. "I'm not going to tell you that cops aren't going to misuse the information."

The most controversial portion of the planned system would be a major expansion to include information on criminal suspects - whose guilt has not yet been established.

The proposed system would include names of persons under investigation in murder, kidnapping or narcotics cases. It would include a so-called "silent hit" feature: An officer in Texas, for instance, would not know that the individual he stopped for speeding was a suspect for murder in Virginia. But when the Virginia investigators flipped on their computer the next morning, it would notify them of the Texas stop. To Michaleski, the proposal sounded like "a great idea. Information is the name of the game."

But the "tracking" ability has angered critics.

"That [data base] could be enlarged into all sorts of threats - suspected communists, suspected associates of homosexuals. There is no end once you start," said Rep. Don Edwards (D-Calif.), whose subcommittee called for the report on the FBI's system.

The FBI's chief of technical services, William Bayse, defends the proposed files, saying they would help catch criminals while containing only carefully screened names. "The rationale is these guys are subjects of investigations, and they met a certain guideline," he said.

So controversial is the suspect file that FBI Director William Sessions reportedly may not include it when he publicly presents his plan for a new system.

[A case similar to Sklar's was reported previously in RISKS -- that of Terry Dean Rogan, who was arrested five times because of outstanding warrants caused by someone else masquerading as him. He finally settled for \$50,000 in damages. PGN]

# Internet mail forgery

<Walter\_Roberson@CARLETON.CA>
Wed, 15 Feb 89 22:14:45 EST

A few days ago, someone forged a message to rec.music.misc. The "From:" address corresponded to that of a gateway for the Apollo mailing list. A couple of people, not recognizing that the fake name corresponded to a mailing list, sent their replies in `privately' instead of to rec.music.misc, with the result that their replies were broadcast whereever the Apollo list and comp.sys.apollo reaches. They were, it seems, subsequently `flamed' for their unintential mis-mailing.

A subsequent note from someone, exposing the message as a forgery, states

> With SMTP and/or NNTP, the forgery could come from anywhere, not > necessarily berkeley or ucsf.

Perhaps someone else can comment on this: can we trust -any- of our (non-encrypted) network mail to be from the claimed author? How about the other way around: how much danger is there that someone can spoof mail in order to receive messages destined for someone else?

Walter Roberson <Walter Roberson@Carleton.CA> (if you can believe that...)

[The simple answer is "no". Furthermore, encrypting the networks does not help very much if the operating systems are vulnerable to attack.

Previous spoofs include "Chernenko at Moskvax" (see ACM SIGSOFT Software Engineering Notes 9 4, July 1984, and last year's "Spafford" hoax. PGN]

## Re: Dead code maintenance

"Clifford Johnson" <GA.CJJ@Forsythe.Stanford.EDU> Wed, 15 Feb 89 18:04:41 PST

My useless code maintenance story concerns a job I applied for once, as a contracted programmer, specifically to maintain one Cobol program. It was billed as a 20-hour per week job, and it's maintenance had kept a Stanford Ph.D. programmer/statistician busy for that amount of time, for some months. (None of this relates to work done at or for Stanford.)

The job was to run the program against fresh data a couple of times a week, and keep the record formats (which rarely changed) up to date. As soon as I reviewed the program, having taken the well-paid job, I discovered that all it did was read-in a file a record at a time, and rewrite some fields from each each record it read-in, without any data change or sorting whatsoever. The second set of records was then read by a statistical program -- which could have read-in the original records directly, simply ignoring the un-needed fields! I contemplated how easy the job was, but recommended scrapping the Cobol program, which not even said Ph.D. had realized was utterly purposeless. This was done - and so I put myself out of work.

I wonder how many programmers do similarly unproductive work because their managers don't realize what is and isn't really being accomplished? Sometimes immediate management knows the score, but instructs one to take more time than needed to make a change. In one employment I was told to take at least two weeks to change the title line in a report, to impress upon senior management how tricky it was and how overloaded we all were.

#### Probabilities and Engines

Steve Philipson <steve@aurora.arc.nasa.gov> Wed, 15 Feb 89 17:50:26 PST

In RISKS 8.26 blinn%dr.DEC@decwrl.dec.com, Dr. Thomas P. Blinn writes:

>In RISKS-FORUM Digest Volume 8 : Issue 24, it is asserted by Barry Redmond that

<>If someone makes a mistake on one engine at any of these times, there is a <>high probability that they will make the same mistake on the other engine(s).

>That may be true, but it may not be true, because the same person may not >be working on all the engines. I would agree that an incompetent mechanic >working on all the engines is likely to make the same mistakes on all of >them, but the reality of aircraft engine repair is different.

There are several well known cases where all engines on a multi-engine aircraft failed (or were in the process of failing) due to the same maintenance error. Sometimes it's the result of a single person's work, and in other cases it's the result of systematic error by a group. The reality is that such errors and failures do occur.

>The probabilities of failure are not independent because if one engine fails it >immediately increases the probability of another failing.

<>This is a very interesting assertion. It seems to be saying that there is a <>causal relationship between a first engine failure and the likelihood of a <>second. ... , but this doesn't mean that the probability of failure of the <>other engines has changed in any way. ...

There is such a causal reationship. When one engine fails, the remaining engine(s) may have to be operated at increased power levels and shoulder additional tasks. This raises the stress on them, and gives us an a priori knowledge of increased probabilty of failure.

It may be necessary to have a thorough grounding in probability theory and statistics, but it is also necessary to have knowledge of the specifics of real world operations. Either without the other sets us up to allow problems to escape detection and analysis.

# Probabilities and Engines

Robert Dorsett <mentat@louie.cc.utexas.edu> Thu, 16 Feb 89 14:56:20 CST

NOTE: a longer version of this tirade will soon appear on USENET's rec.aviation... I'll mail a copy to anyone without usenet access.

#### Jordan Brown wrote:

>727 engines (3/airplane) are wimpy compared to DC-9 engines (2/airplane).
>BAe-146 engines (4/airplane) are \*really\* wimpy. (This assumes that
>727s are approximately the same size as DC-9s. Bae-146's are smaller.)

The 727 and DC-9 engines are the same, derivatives based on the Pratt & Whitney JT8D. What is significant, in the context of this discussion, is how the engine thrust relates to the airplane weight. Here are a few thrust-to-weight ratios, assuming various weights and engine-remaining situations:

727-200,000 lbs (max) 727-200, 140,000 lbs DC-9-30,140,000 lbs (max)

3 2	4:1	3:1	
	6:1	5:1	4:1
1	13:1	9:1	9:1

One can change the performance of an airplane by losing weight; to lose weight, fuel is dumped. The 727 can lose some 60,000 lbs of fuel. The one-engine case with no fuel is a performance increase of some 30% over the same thrust at max.weight.

To give an example of the significance of all this, recently a fully-loaded Continental 747, enroute to New York, attempted to take off from Gatwick, heading north. It had an engine fire and shutdown at takeoff. The pilot was just barely able to hold altitude after takeoff (with three engines), at 200-300 feet, with the stick shaker and stall warnings active. The airplane went behind some trees; the controller called a crash after losing radar and visual contact. The plane dumped a massive amount of fuel, managed to gain altitude (after several minutes), and returned to the field.

The moral here, again, is that from the mundane perspective of keeping the airplane in the air, it's not how many engines you have, but how much you weigh. What is far more important for trans-oceanic operations is how likely it is to lose some or all of your engines, and how likely it would be to get to an airfield once you do. Considering the frequency with which total (or near-total) freakish engine failures have occurred the last few years (even though the engines themselves are more reliable than in the past), this isn't really as trivial or as "safe" as the numbers might have us believe.

>Airplanes are required to be >able to maintain such-and-such a level of performance with one engine out.

The most important situation normally considered being takeoff. I doubt a 727 could take off with two engines out; it wouldn't have the time necessary to dump, or the thrust necessary to maintain airspeed. As the above 747 example shows, even the worst-case performance figures can be misleading. At the end of the flight, that same 747 would be able to perform with only one engine operating (as a recent United Airlines emergency landing on a flight to Tokyo showed).

>I don't believe a 727 can fly on one engine. It must have two.

It can fly on one engine. And even if it couldn't fly on one engine, as another poster pointed out, having \*any\* thrust means the difference between a steep glide and a long glide. According to the 727 patterns manual, a one-engine ILS approach is made by assuming a decision height of some 600 feet, with an airspeed in the 160-170 kt range. Best climb speed, for the go-around, is 200 kts (190 knots with two degrees of flaps). There's an implicit assumption in the training manual that between 600 feet and ground level, they will be able to accelerate--and hold--200 kts.

>A three-engine airplane has a higher probability of having a failure in

>the first place, and when it does have a failure it then has two points >of failure, EITHER of which will cause an accident.

The 727 has three engines because, more than any other factor, Boeing perceived a need to trade off airline requirements at the time the plane was constructed. United Airlines wanted a four-engine airplane, Eastern wanted two. So they compromised, and agreed on three. I suspect a similar history with the Tristar and DC-10: four is too many, two is too few. Three is nice and "safe."

>Going from one engine to two adds redundancy. Going from two to three, >with two required, REDUCES redundancy.

Perhaps we should look up the meaning of "redundancy." Three engines provide three thrust sources, three generators, three pneumatics sources, and (on the 727) two hydraulic sources. I can't imagine how that is "bad," since (apart from fuel starvation, mismanagement, and particle ingestion) they really don't have a common failure mode. There are more parts to fail, but the issue here is whether more engines will make it more likely for everything to go wrong in a catastrophic manner, which years of experience has shown to be fallacious.

Robert Dorsett

# ★ Re: Aircraft failures (RISKS DIGEST 8.26)

<dag@fciva.UUCP> Thu, 16 Feb 89 16:52:04 -0500

First, there seems to be some disagreement on the subject. Does anyone have any information on the capability of currently popular 3-engine commercial aircraft (DC10, L1011, B727) to maintain level flight with only one functioning engine?

Second, to expand upon the comments of Dr. Blinn, my recollection of statistics is as follows:

Each engine has its own (unknown) probability of failure during any time interval. This probability is a function of many known and unknown factors (history, current aircraft state, fuel, maintainence, etc.). Initially, we have an ESTIMATE of this probability which is the same for all engines: some sort of historical average or other statistic. The failure of one engine on an aircraft gives additional information regarding those factors which are common, and thus allows us to revise our estimate of the probabilities of another failure on the same aircraft in the near future.

Normally, a statistician would say that the probability of failure hasn't changed, just our estimate. There is an exception to this statement. It is possible that the failure of the first engine is itself a factor in the failure of the second, for example, by increaseing the load that engine is run under, or stress on the aircraft from unequal thrust.

I think the most misunderstood aspect of statistics is that probability distributions for real world phenomena are rarely known, only estimated. The march of time gives us new information to refine our estimates.

Dan Graifer

The usual disclaimers....

Daniel A. Graifer, Franklin Capital Investments,

7900 Westpark Drive, Suite A130, McLean, VA 22102 (703)821-3244



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 8: Issue 28

# Sunday 19 February 1989

## **Contents**

- Continuing problems with WWMCCS command-and-control network Jon Jacky
- US missile-warning radar endangers friendly aircraft Jon Jacky
- Power failure problems

John Sinteur

The Risks of Going on Vacation

Jim Carson

Re: Faking Internet mail

Peter Scott

Multi-gigabuck value of information theft denied

Mark Brader

Re: multi-gigabuck information "theft"

**David Chase** 

Re: Authenticity in digital media

**Doug Krause** 

Digital doctoring of images

**Richard Wiggins** 

PIN? Who needs a PIN?

**Bill Mahoney** 

Info on RISKS (comp.risks)

# ✓ Continuing problems with WWMCCS command-and-control network

Jon Jacky <jon@june.cs.washington.edu> 17 Feb 1989 09:25:29 EST

The following excerpts are from GOVERNMENT COMPUTER NEWS Feb. 6, 1989 p.1:

AF MAY LOSE WIS PROJECT - DCA LIKELY TO TAKE OVER GLOBAL SYSTEM by Brad Bass

Officials in the Office of the Secretary of Defense (OSD) planned to meet late last week to consider transferring responsibility for procuring an upgraded Worldwide Military Command and Control System (WWMCCS) from the Air Force to the Defense Communications Agency. ...

Glenwood Stevener, director of DCA's Joint Data System Support Center, said the Air Force's WWMCCS Information System (WIS) program was a victim of a vicious circle of schedule slippage and budget cuts. "These things feed on each other," he said.

WWMCCS began in the late 1970's as an effort to provide the president, the Defense secretary, the Joint Chiefs of Staff and other military authorities with information to help them make wartime decisions.

When a study later that decade showed the system was too slow and limited, officials launched the WIS upgrade project.

The Air Force has suffered several setbacks since being selected in 1982 to manage WIS. In July 1987, the WIS program office announced the system would be delayed about a year due to funding cuts and system development problems.

A year ago the General Accounting Office reported that program officials had not adequately defined system requirements and security measures. Subsequent funding problems delayed the project by another 12 months to 15 months.

Air Force officials who requested anonymity said OSD officials recently set up a task force to propose alternative methods to upgrade WWMCCS in light of WIS program difficulties. ...

DCA would take more of an ``evolutionary'' approach to the upgrade than the Air Force did, Stevener said. He said the Air Force has been attempting to field a turnkey system to fulfill a broad range of WWMCCS requirements. The DCA plan would focus on a fielding a partial system at first and incrementally adding capabilities to it, he said.

In addition, Stevener said DCA would probably change the name of the program to differentiate it from WIS.

- Jonathan Jacky, University of Washington

## US missile-warning radar endangers friendly aircraft

Jon Jacky <jon@june.cs.washington.edu> Fri, 17 Feb 89 10:07:17 PST

These are excerpts from THE NEW YORK TIMES, Feb 12, 1989, p. 14:

ADEFENSE RADAR MUST TURN OFF AS PLANES LAND - AIR FORCE FEARS SYSTEM COULD TRIGGER A BLAST (no author given)

WASHINGTON, Feb. 11 (AP) - For 14 months operators of a huge radar installation in central Georgia that is part of the United States' defense warning system have had to turn off the system while military aircraft

landed at a nearby base.

The interruptions are to avoid accidental detonations of tiny explosive charges found in virtually every military weapons system and in the planes and ships that deliver them.

The charges are used, among other things, to trigger weapons, drop bombs or jettison fuel tanks. They are normally fired by an electrical circuit, bu they can also be set off by high levels of electromagnetic energy from such sources as radio waves, static electricity, lightning or radar.

As a result, the powerful radar center has to be turned off periodically so planes can land safely at Robins Air Force Base, two miles to the north.

That precaution is not enough, local critics contend. They fear a major accident at the air base and have sued to force safety improvements.

#### INTENDED TO SPOT MISSILES

The \$90 million radar complex, on of four of its type in the United States, would provide instant warning of a submarine-launched missile off the southeast coast [The story does not say so, but I believe this must be one of the PAVE PAWS phased-array radar intallations - JJ ].

Th Air Force says the unit's time out of service caused by landing planes totals about an hour a month. Ther interruptions have not hindered the early warning system, the Air Force says, because they are random and other radars are available as backups. Routine maintenance of the system turns the radar off for about 40 hours a month, an official said.

The 10-story, pyramid shaped installation consists of thousands of antennas that can scan 240 degrees for 3,000 miles and can reportedly identify an object the size of a basketball 1,500 miles away.

### CRITICS FEAR A DISASTER

(Robins Air Force Base) is Georgia's largest and is near the city of Warner-Robins, which has a population of 40,000. ... Critics have filed a lawsuit in Federal Court in Washington.

Patricia Axelrod, coordinator of one of the groups that has joined in the suit ... argues that flight restrictions force pilots into`` a trapeze act without a net" because of the possibility of an error in the communication required to turn off the radar.

Senator Sam Nunn, the Georgia Democrat who is chairman of the Senate Armed Services Committee, has also criticized the restrictions because of their reliance "on the potentially fallible human links" required to turn the system off.

## **OPTIONS BEING CONSIDERED**

The Air Force has already spent \$600,000 for a study by the Raytheon Corporation, which built the radar system. The study recommended moving it,

at a cost of \$37.7 million, or modifying it, at a cost of \$27 million, so it would turn off automatically if a plane breached the restricted zone.

Lieut. Gen. Donald J. Kutyna, who heads the Air Force Space Command that has jurisdiction over the unit, said moving it is not reasonable but modification remains under consideration. A decision is to be made in June.

[I find several things interesting about this story, apart from the overall irony of the situation. First, it is another illustration of the tendency noted by Paul Bracken and others for modern military C3I systems to become ever-more tightly-coupled and interdependent in ways unforseen by their designers. Second, Nunn and others' assumption that some kind of automated system would necessarily be more reliable than the present arrangement.

- Jon Jacky, University of Washington ]

## Power failure problems

<ADEGROOT@HROEUR5.BITNET> Sun, 19 Feb 89 13:38 N

I ran into something curious when I visited my previous employer yesterday. They moved to a brand new building recently, and took the opportunity to increase access-security. They installed magnetic card readers on all doors (including the computer-room doors), keeping physical access to the office space and the computer room under control in a better way.

They thought.

A few days after the move, the power went down. The UPS cut in, and kept the computer systems on juice. The operators have got 15 minutes to manually turn off the computer systems (after software shutdown procedures of course) before the batteries are out as well. Unfortunately, the card readers were out, making it very difficult indeed to enter the computer room...

No need to say that they modified the system a bit...

It's small things like this that are difficult to anticipate, but are sooooo important...

-John Sinteur

Whatever I say is not to be taken as a statement of the Dutch Army (my current employer) or my previous employer who shall remain nameless here.

## The Risks of Going on Vacation

Jim Carson <carson@rice.edu> Sun, 19 Feb 89 12:06:31 CST

I was going to be out of town and wanted to use "vacation." For those who aren't familiar with it, vacation is a program from 4.[23]BSD that sends a form letter back to anyone who sends you mail. This is useful because you can let people know when you will return and give them other ways to contact you in an emergency.

Vacation has provisions so you don't send mail to MAILER-DAEMON, Postmaster, or a \*-Request@\*, since these senders are usually automated and you could risk getting into a mail-loop if you sent form-letters back.

Now consider what would happen if you subscribed to an automated discussion group that sends mail without any of these lines in the header. This was the case with Sun-Spots, the Sun discussion group moderated by Bill LeFebvre at Rice. The header:

- > From SUNSPOTS@icsa.rice.edu Sun Feb 19 09:42:43 1989
- > Reply-To: SUN-SPOTS%RICE.EDU@icsa.rice.edu
- > Sender: Sun Spots Discussion <SUNSPOTS%RICE@icsa.rice.edu>

The discussion group was set up so when Bill is done compiling an issue, he sends it to a mail alias containing a list of everyone who subscribes to Sun-Spots. When I got a copy of the issue, vacation sent a reply. However, since the reply goes to everyone who subscribes to the group, including myself, a reply to the reply was sent, and so on.

About forty messages were sent before I logged in this morning to check for any last minute mail. One of the other subcribers sent me mail because he thought we had a mail virus. [...]

# ★ Re: Faking Internet mail [Re: RISKS-8.27]

Peter Scott <PJS@grouch.JPL.NASA.GOV> Fri, 17 Feb 89 10:07:19 PDT

It is incredibly easy to fake mail. Read RFC 821, which although it is 50 pages long, details on page 4 everything you need to know. The server on the first remote machine (that which comes after "@") expects to see commands of the form:

HELO (optional)

MAIL From: <reverse-path>
RCPT To: <forward-path>

DATA

## Multi-gigabuck value of information theft denied

Mark Brader <msb@sq.sq.com> Fri, 17 Feb 89 12:07:19 EST

A few days ago I summarized for RISKS an article that had appeared in the Toronto Star on February 8 about a case of "theft" of information. [...]

Two days later, however, significantly different facts were reported. (This submission to Risks was delayed because I intended to email to

Mike Tilson to ask if he wanted to write something himself.)

Information here is from the (Toronto) Globe & Mail. The article is headlined "Computer information theft detected by security system, company says". And it begins as follows:

- # The theft of information from a company's computer program [sic]
- # was detected by the firm's own computer security system.

#

- # Mike Tillson [sic], president of HCR Corp., which specializes in
- # developing computer software, said yesterday an unusual pattern
- # of computer access was noticed on the company's system last week.

The article continues by saying that police reports valuing the "program" at \$4 billion (Canadian) were called grossly exaggerated by Tilson: "It's more in the tens of thousands of dollars range". He also said that the illegal access had been only a week before; there was no 2-month investigation. And asked about resale of the information , he said: "It's not clear how one would profit from it. There are any number of purposes one could imagine to idle curiosity. There is a possibility of no criminal intent."

The information not being HCR customer data, and Tilson declining to identify it, the article goes on to mention UNIX, to mumble about AT&T intellectual property, and to note that AT&T is not in the investigation "at this stage".

Mark Brader "Every new technology carries with it SoftQuad Inc., Toronto an opportunity to invent a new crime" utzoo!sq!msb, msb@sq.com -- Laurence A. Urgenson

## Re: multi-gigabuck information "theft"

David Chase <chase@orc.olivetti.com> Thu, 16 Feb 89 12:11:44 -0800

In RISKS 8.26, Jeff Makey says:

- > The "computer files" are nothing more than the source
- > code for AT&T's UNIX operating system ... few thousand dollars --
- > a far cry from \$4 billion. I suspect that AT&T's lawyers are at
- > the root of this sensationalism.

I think in this case the lawyers are doing their job, and it might not be sensationalism. I believe (word of mouth from UNIX-related legal mess that some friends were in long ago) that the UNIX operating system is protected by trade secret law, and (according to my copy of \_Legal Care for Your Software\_) a corollary of this is that you must diligently maintain the "secret" (licensed, confidential) status of that software, or all your legal protection is gone. If the lawyers don't behave like rabid piranhas, then perhaps they aren't being diligent, and if they aren't diligent and lose trade secret protection, then the loss to AT&T could well total billions.

And, of course, since we're talking about product protection, "UNIX" is a

trademark of AT&T.

**David Chase** 

# ★ Re: Authenticity in digital media [RISKS-8.26]

Doug Krause <dkrause@ORION.CF.UCI.EDU> 17 Feb 89 11:39:37 GMT

"ALBTSB::SCHILLING1" <schilling1%albtsb.decnet@aldncf.alcoa.com> writes:

>Seeing hasn't been believing for a long time. Remember Fred Astaire dancing on >the ceiling in the movie "Singing in the Rain"?

Gene Kelly was in "Singing in the Rain". Fred Astaire's ceiling dance was in "Royal Wedding".

Douglas Krause, University of California, Irvine

[Also noted by cmb@robots.oxford.ac.uk (Chris Brown).]

# Digital doctoring of images (re Steve Philipson, RISKS-8.25)

<Richard\_Wiggins@um.cc.umich.edu>
Thu, 16 Feb 89 09:33:00 EST

Steve Philipson points out the risks of new technologies to digitally alter video images and audio recordings. An article in The Whole Earth Review about three years ago discussed the digital doctoring of photographic (still) images; that technology is quite mature already. The article pointed out that the major news publishers such as Time own digital processing devices that put the best airbrush artist to shame. It is quite easy to merge unrelated images, superimposing a person in a scene he never visited, and to cover all the seams. It is also easy to remove unwanted objects and blend in the background to cover.

The claim in this article was that photographic images were no longer worthwhile as evidence of anything. I suspect that is a bit strong; the testimony of a photographer that her record is honest would probably hold water. (After all, the notes of a police officer can be altered, but are admissable when read as part of testimony.) Also, few currently have direct access to this technology.

But the risks are real.

# ✓ PIN? Who needs a PIN? (Alan Wexelblat, RISKS-8.26)

<bill%zycor%ugn%hdr%mcmi%uunet@ames.UUCP>
Sat, 18 Feb 89 01:10:44 -0500

Like most ATMs, the Diebolds (there are several models) are programmable from the host computer. This can include modes where the pin is read and encrypted (DES) before sending, or where the PIN is read and sent in the clear, or where the pin is not even read. It would seem a little strange to run the ATM in the last mode, but I have seen a system in the UK where the PIN is transmitted over a bisync line with no encryption whatsoever. In any case, the menus, the "fast \$xx" amount, the order of operations when processing a user transaction, etc. are all remotely programmable. It could be that the ATM you were at had been incorrectly programmed, but generally there is one file in the host that contains the ATM information, and this is just sent down over the wire to all of them. Your name was probably encoded on track 1 or 3 of the card.

[That does open up some significant vulnerabilities. PGN]

On a related note, I noticed quite a risk using credit cards. We are currently implementing a credit card (CC) authorization system for retail stores, and the handy way to test it seemed to be to run my own card through the magnetic reader. Now, a CC has a "track two" where the account information is encoded. After the account information, there is a special character that serves as a field sep, and then "issuing bank discretionary data" follows. In this field the first four are usually the expiration date on the card. In the case of Commercial Federal here in Omaha, my checking account is there, AND it is the issuing bank for my CC. Imagine my suprise when testing the card reader with my CC. The CC account is there, so is the expiration date, followed immediately by MY CHECKING ACCOUNT NUMBER at Commercial Federal! So apparently my bank account number is going over the wire every time I buy something with my Visa...

Bill Mahoney



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 8: Issue 29

# Wednesday 22 February 1989

# **Contents**

- Overloaded computer delays (overworked) commuters **Steve Graham**
- Chicago Phone Freak Gets Prison Term Patrick Townson via Cliff Stoll
- Computer Confinement Joseph M. Beckman
- Police officers sentenced for misuse of PNC **Nigel Roberts**
- The word "virus" causes panic
- **Nigel Roberts** Re: Faking Internet mail
- Steve Bellovin Kevin S. McCurley
- Info on RISKS (comp.risks)

# Overloaded computer delays (overworked) commuters

<Owen Plowman <owen@oracle.com> [Really Steve Graham]> Tue, 21 Feb 89 14:31:14 EDT

This message actually comes to you from Steve Graham (sgraham@cnseq1.oracle.com), and not from me (Owen Plowman).

You might find this interesting. It is a 'COMMUTER BULLETIN' published by Government of Ontario [GO] Transit. I and everyone using the system was affected by it.

[GO Transit trains serve a wide area around Toronto, transporting commuters between the downtown area and surrounding communities. I believe that the trains are operated for the Provincial Government by Canadian National Railways]

February 15, 1989

#### SIGNAL COMPUTER DELAYS RUSH-HOUR GO TRAINS

Homebound GO Train riders were subjected to delays of up to 80 minutes on Monday and Tuesday evenings.

The delays were caused by a shortage of capacity in the new computer recently installed by CN Rail to control the signalling on its main line between Toronto and Hamilton. In the late afternoon, this line is heavily used over its entire length, and the computer has not been able to process signal and routing requests as rapidly as the traffic requires.

GO's Lakeshore trains use this line and were seriously affected. Also delayed were trains on the Milton, Georgetown, Bradford and Stouffville lines, whose equipment encountered the signal problems between Union Station and GO's maintenance facility in Mimico. Compounding the delays were several locomotive malfunctions as well.

CN hopes to have the computer problem solved by the end of this week. In the meantime, the railway is altering its operating procedures in order to minimize further impact on GO riders.

GO apologizes for this inconvenience.

Steve Graham, Oracle Corporation Canada, Toronto, Ontario, M5J 2M4 Opinions expressed in this message are those of the author.

## Chicago Phone Freak Gets Prison Term

Cliff Stoll <cliff%cfa204@harvard.harvard.edu> Mon, 20 Feb 89 01:36:57 est

From: telecom@eecs.nwu.edu (TELECOM Moderator) [From Patrick Townson]

Newsgroups: comp.dcom.telecom

Subject: Chicago Phreak Gets Prison Term

Date: 17 Feb 89 06:47:45 GMT

X-TELECOM-Digest: volume 9, issue 65, message 1 of 5

An 18 year old telephone phreak from the northside/Rogers Park community in Chicago who electronically broke into U.S. military computers and AT&T computers, stealing 55 programs was sentenced to nine months in prison on Tuesday, February 14 in Federal District Court here.

Herbert Zinn, Jr., who lives with his parents on North Artesian Avenue in Chicago was found guilty of violating the Computer Fraud and Abuse Act of 1986 by Judge Paul E. Plunkett. In addition to a prison term, Zinn must pay a \$10,000 fine, and serve two and a half years of federal probation when released from prison.

United States Attorney Anton R. Valukas said, "The Zinn case will serve to demonstrate the direction we are going to go with these cases in the future. Our intention is to prosecute aggressively. What we undertook is to address the problem of unauthorized computer intrusion, an all-too-common problem that is difficult to uncover and difficult to prosecute..."

Zinn, a dropout from Mather High School in Chicago was 16-17 years old at the time he committed the intrusions, using his home computer and modem. Using the handle 'Shadow Hawk', Zinn broke into a Bell Labs computer in Naperville, IL; an AT&T computer in Burlington, NC; and an AT&T computer at Robbins Air Force Base, GA. No classified material was obtained, but the government views as 'highly sensitive' the programs stolen from a computer used by NATO which is tied into the U.S. missle command. In addition, Zinn made unlawful access to a computer at an IBM facility in Rye, NY, and into computers of Illinois Bell Telephone Company and Rochester Telephone Company, Rochester, NY.

Assistant United States Attorney William Cook said that Zinn obtained access to the AT&T/Illinois Bell computers from computer bulletin board systems, which he described as '...just high-tech street gangs'. During his bench trial during January, Zinn spoke in his own defense, saying that he took the programs to educate himself, and not to sell them or share them with other phreaks. The programs stolen included very complex software relating to computer design and artificial intelligence. Also stolen was software used by the BOC's (Bell Operating Companies) for billing and accounting on long distance telephone calls.

The Shadow Hawk -- that is, Herbert Zinn, Jr. -- operated undetected for at least a few months in 1986-87, but his undoing came when his urge to brag about his exploits got the best of him. It seems to be the nature of phreaks that they have to tell others what they are doing. On a BBS notorious for its phreak/pirate messages, Shadow Hawk provided passwords, telephone numbers and technical details of trapdoors he had built into computer systems, including the machine at Bell Labs in Naperville.

What Shadow Hawk did not realize was that employees of AT&T and Illinois Bell love to use that BBS also; and read the messages others have written. Security representatives from IBT and AT&T began reading Shadow Hawk's comments regularly; but they never were able to positively identify him. Shadow Hawk repeatedly made boasts about how he would 'shut down AT&T's public switched network'. Now AT&T became even more eager to locate him. When Zinn finally discussed the trapdoor he had built into the Naperville computer, AT&T decided to build one of their own for him in return; and within a few days he had fallen into it. Once he was logged into the system, it became a simple matter to trace the telephone call; and they found its origin in the basement of the Zinn family home on North Artesian Street in Chicago, where Herb, Jr. was busy at work with his modem and computer.

Rather than move immediatly, with possibly not enough evidence for a good, solid conviction, everyone gave Herb enough rope to hang himself. For over two months, all calls from his telephone were carefully audited. His illicit activities on computers throughout the United States were noted, and logs were kept. Security representatives from Sprint made available notes from

their investigation of his calls on their network. Finally the 'big day' arrived, and the Zinn residence was raided by FBI agents, AT&T/IBT security representatives and Chicago Police detectives used for backup. At the time of the raid, three computers, various modems and other computer peripheral devices were confiscated. The raid, in September, 1987, brought a crude stop to Zinn's phreaking activities. The resulting newspaper stories brought humiliation and mortification to Zinn's parents; both well-known and respected residents of the Rogers Park neighborhood. At the time of the younger Zinn's arrest, his father spoke with authorities, saying, "Such a good boy! And so intelligent with computers!"

It all came to an end Tuesday morning in Judge Plunkett's courtroom here, when the judge imposed sentence, placing Zinn in the custody of the Attorney General or his authorized representative for a period of nine months; to be followed by two and a half years federal probation and a \$10,000 fine. The judge noted in imposing sentence that, "...perhaps this example will defer others who would make unauthorized entry into computer systems." Accepting the government's claims that Zinn was 'simply a burglar; an electronic one... a member of a high-tech street gang', Plunkett added that he hoped Zinn would learn a lesson from this brush with the law, and begin channeling his expert computer ability into legal outlets. The judge also encouraged Zinn to complete his high school education, and 'become a contributing member of society instead of what you are now, sir...'

Because Zinn agreed to cooperate with the government at his trial, and at any time in the future when he is requested to do so, the government made no recommendation to the court regarding sentencing. Zinn's attorney asked the court for leniency and a term of probation, but Judge Plunkett felt some incarceration was appropriate. Zinn could have been incarcerated until he reaches the age of 21.

His parents left the courtroom Tuesday with a great sadness. When asked to discuss their son, they said they preferred to make no comment.

Patrick Townson

## Computer Confinement

"Joseph M. Beckman" <Beckman@DOCKMASTER.ARPA> Wed, 22 Feb 89 07:54 EST

[Joseph included an article From the Washington Times (2-16-89) and commented thusly:]

It is interesting that the judge wants this person to reform with computers. One would find it incongruous to direct, say, an alcoholic to work in a liquor store (a legal outlet), or an embezzler to work in another financial institution, etc. Perhaps the penalty or terms of probation should call for the abuser to stay away from that which he is abusing or using to break the law.

Joseph

[Article also noted by Rodney Hoffman < Hoffman. El Segundo @ Xerox.com >.]

## Police officers sentenced for misuse of PNC

Nigel Roberts <roberts%untadh.DEC@decwrl.dec.com> Mon, 20 Feb 89 02:48:11 PST

#### SUSPENDED SENTENCES FOR COMPUTER BREAK-IN

Three police officers hired by private investigators to break into the Police National Computer received suspended prison sentences at Winchester Crown Court. The private investigators also received suspended (prison) sentences, ranging from four to six months.

The police officers were charged under the Official Secrets Act of conspiring to obtain confidential information from the Police National Computer at Hendon.

One of the police officers admitted the charge, but the other two and the private investigators pleaded Not Guilty.

The case arose out of a TV show called \_Secret Society\_ in which private investigator Stephen Bartlett was recorded telling journalist Duncan Campbell that he had access to the Police National Computer, the Criminal Records Office at Scotland Yard and the DHSS [Department of Health & Social Security --nr] computer.

Bartlett said he could provide information on virtually any person on a few hours. He said he had the access through certain police officers at Basingstoke, Hampshire. Although an investigatation proved the Basingstoke connection to be false, the trail led to other police officers and private detectives elsewhere.

Most of the information gleaned from the computers was used to determine who owned certain vehicles, who had a good credit record -- or even who had been in a certain place at a certain time for people investigating marital infidelity.

-- From \_Personal Computing Weekly\_ dated 9/15-Feb-1989.

[Of course, the actions for which the officers and others were sentenced, were not computer break-ins as such, but rather misuse of legitimate access.

It seems the phrase "break-in", applied to computers, is almost as fashionable as "virus" with the media at the moment --nr]

## ★ The word "virus" causes panic

Nigel Roberts <roberts%untadh.DEC@decwrl.dec.com> Mon, 20 Feb 89 02:41:19 PST

#### VIRUS HOAX CAUSED AS MUCH PANIC AS THE REAL THING

Sixth-form student [high-school--nr] and \_Popular Computing Weekly\_ reader Michael Banbrook gave his college network managers a scare when he planted a message saying that a virus was active on the college system.

Banbrook's message appeared whenever a user miskeyed a password; the usual message would be

"You are not an authorised user".

It was replaced by the brief but sinister:

"A Virus is up and running".

When the message was discovered by the college network manager, Banbrook was immediately forbidden access to any computers at the St. Francix Xavier Collegs at Clapham in South London.

Banbrook, 17, told \_Popular Computing Weekly\_ that he believed the college has over-reacted and that he had, in fact thrown a spotlight on the college's lacklustre network security. The college has a 64 node RM Nimbus network running MS-DOS.

"All any has to do is change a five-line DOS batch file" says Banbrook. "There is no security at all"

Banbrook admits his motives were not entirely related to enhancing security: "I was just bored and started doodling and where some people would doodle with a notepad, I doodle on a keyboard. I never thought anyone would believe the message"

Banbrook was suspended from computer science A-level classes and forbidden to use the college computers for a week before it was discovered that no virus existed. Following a meeting between college principal Bryan Scalune and Banbrook's parents, things are said to be "back to normal".

-- from Popular Computing Weekly dated 9-15/Feb/89

[I think there are several lessons here. The college seems to have been using networked PCs without realising that how an informed ordinary user could change system messages for everyone on the network. The student himself doesn't seem to have been aware of the possible consequences of his "doodling" (echoes of the discussion of the need to educate people about ethics and "proper use"), and of course it is highly revealing to note the knee-jerk way everone reacted when they saw the currently fashionable buzz-word "virus" on their screens --nr]

★ Re: Faking Internet mail [Re: RISKS-8.27]

<smb@research.att.com>
Sun, 19 Feb 89 21:10:07 EST

Yes, it's just as easy to fake netnews articles. In fact, if you're a bit careful, you can not only spoof someone, you can arrange things so that the victim doesn't even see the forged article.

Back when we were designing the original protocols, we discussed the security issue. Since we were using a completely unauthenticated transport medium (uucp), at least as far as the application layer was concerned, we felt that there could be no real security; consequently, we elected to omit all control messages. That decision was subsequently changed by later implementors, and there have indeed been a few problems, albeit mostly inadvertent. But the first public release of "B netnews" had some very serious security problems indeed; a forged control message could be used to remove every file belonging to the owner of netnews. In the best case, that was "merely" every stored netnews article; in the worst case -- some implementation quirks in thencurrent versions of the UNIX system -- the recursive remove command would run as root, and could wipe the entire file system.

I don't remember why we didn't adopt a public-key system during the initial design phase; we certainly knew about them, and even had some code (the V7 xsend/xget commands) to model ours on. Most likely, we didn't see the need; we expected a maximum size of 50-100 sites, and 1-2 messages/day.

--Steve Bellovin

# Faking Internet mail

"Kevin S. McCurley" <mccurley@IBM.com> Sun, 19 Feb 89 22:15:54 PST

I guess a lot of people know about faking internet mail. Since the National Science Foundation now accepts reviews of proposals via email, I wonder whether anybody there knows about this? It is rather farfetched to think that somebody would try to fake their reviews, but I wonder if there are many other examples where individuals or organizations are leaving themselves open to fraud this way...

Kevin McCurley, IBM Almaden Research Center



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 8: Issue 30

# Friday 24 February 1989

# Contents

"Do you know who's reading your medical records?"

Wells Fargo ATM outage **PGN** 

New York 540 Phone Number Scam

John Murray 900 "confession" number

Randal L. Schwartz

Re: Chicago Phone Freak Gets Prison Term Rich Salz

Reach Out and Spy on Someone

Peter Scott

Power failure problems Jonathan I. Kamens

Photographs as evidence (re: digital editing, etc.) Ernest H. Robl

Stanford and rec.humor.funny

**Martin Minow** 

Info on RISKS (comp.risks)

# ✓ "Do you know who's reading your medical records?"

Peter Neumann < neumann@csl.sri.com> Fri, 24 Feb 1989 11:18:27 PST

Of considerable interest to RISKSers is an article entitled "Absolutely NOT Confidential" by Clark Norton, in the March/April 1989 issue of Hippocrates (The Magazine of Health and Medicine). The article documents many of the problems of large networked databases, including privacy, data quality, legal and social implications, etc. It also includes a state-by-state table on your access to your own medical records, with separate entries for doctors', hospitals', and mental health records. Arkansas, New Hampshire, Rhode Island, South Carolina, Vermont, and Wyoming are the only states left with no laws guaranteeing your access for all three types of records. Thus far, Montana is

the only state to adopt a model bill drafted by the National Conference of Commissioners on Uniform State Laws.

"Like most Americans, you've probably assumed your medical records were confidential -- protected by ethics and the law. At one time you would have been right. "We used to have a medical system that was confidential," says retired Harvard School of Medicine neurosurgeon Vernon Mark..." Now it is relatively wide open.

# ✓ Wells Fargo ATM outage

Peter Neumann <neumann@csl.sri.com> Fri, 24 Feb 1989 11:02:52 PST

445 of Wells Fargo's 1200 ATMs in California were out of commission for many hours on 22 Februrary 1989, due to computer malfunctions. (Bank of America has twice had about 700 ATMs out of commission in recent months.)

'John Love, publisher of Bank Network News, a newsletter that covers electronic banking, said that, on the average, ATMs are down 5 percent of the time because of ``machine-specific problems." However, such widespread failures are rare, he said, because of extensive backup computer networks.' [Quote from the San Francisco Chronicle, 23 Feb 89, pp. C1 and C18, in an article by David Tuller.]

### New York 540 Phone Number Scam

John Murray <johnm@uts.amdahl.com> 24 Feb 89 02:31:46 GMT

Just picked this up from comp.dcom.telecom - John Murray , Amdahl Corp., Sunnyvale, CA.

From wrf@ecse.rpi.edu Tue Feb 21 07:50:32 1989 Subject: 540 ripoff

NYS just fined a ripoff outfit that advertised a "GOLD" card if you called 540-GOLD. Several hundred people who did, and stayed on the line for a minute, were billed \$50 (FIFTY DOLLARS). Needless to say their gold card had no relation to Mastercard or Amex. They were also contacting people with an illegal autodial operation that would not let the victim hang up to free the line. I think now they're required to say at the start of the call that there is this charge. But what about people whose hearing is bad or English poor?

People in every state should have the right to disable this use of their phone as a no limit credit card. In fact, the default status should be disabled, and phone customers should have to enable it, and perhaps specify a \$limit, if they want to use it.

[Moderator's Note: Illinois Bell was one of the first telephone companies to offer 900/976 blocking at no charge, no questions asked. We do not have

'540' service here -- yet -- but I assume any variation on it here would get free blocking. Here you can block 976 or 900 or both. The operator is unable to complete the connection for you. Out-of-LATA 976 calls cannot be blocked, but then they are only billed at regular long distance rates anyway. PT]

## ✓ 900 "confession" number

Randal L. Schwartz <merlyn@intelob.intel.com> Wed, 22 Feb 89 10:19:15 PST

(Quotes are from an article in the Feb 27 "Insight on the News" magazine)

The latest craze is a 900 number in which callers can "confess" their actions.

Another of those adult phone lines, you think, and prepare to hang up. But then there is another voice, female, young, and remorseful. "I'm having an affair with Bob. He's my boss, and I just gave up our baby," she says. "I want to tell Ginne and Les to please take care of her and I hope that she grows up to be better than I was and [pause] I'm sorry."

[...] Confessors leave a 60-second message on what amounts to an elaborate answering machine, then the tape is edited for playback on the other phone line. Sometimes listeners call in to respond to someone's confession, and some of these calls are played back.

Now, here's the scary part...

Denton [producer of the Phone Confessions program] listens to every call, then selects a mix of confessions for playback. Most calls are about relationships, but United Communications [the producer's company] makes no secret that it gets calls from people confessing to crimes [!!].

Most people probably still believe that the phone number from which they make a phone call is available \*only\* to a select few. But with the 800 and 900 phone services (discussed either in RISKS or TELECOM, I lost track :-), a service-provider can obtain \*instantly\* the caller's phone number, and correlate it with the confessions.

The risks to the public (out of ignorance) is obvious. Law enforcement agencies, or even private opportunists, could set up such services, or tap into existing services, and obtain an unending supply of useful information. Says the article:

Denton believes that 98 percent of her calls are true confessions.

I suppose if I really wanted to confess a crime to one of these services, I'd go to a pay phone. I doubt that the public is aware of the consequences of calling from their home, though.

Randal L. Schwartz, Stonehenge Consulting Services (503)777-0095 on contract to BiiN (for now :-), Hillsboro, Oregon, USA.

# ★ Re: Chicago Phone Freak Gets Prison Term (RISKS 8.29)

Rich Salz <rsalz@BBN.COM> 23 Feb 89 00:19:10 GMT

>... and the Zinn residence was raided by FBI agents, AT&T/IBT security >representatives and Chicago Police detectives used for backup.

ATT security people as backup? "Stop right there, this is the phone company; hands against the wall!" Is it common practice in such "raids" to use outside companies?

# ✓ Reach Out and Spy on Someone

Peter Scott <PJS@naif.JPL.NASA.GOV> Thu, 23 Feb 89 10:41:46 PST

An article in \_Digital Review\_, February 20, under the title "Reach Out And Help Someone" reviews a package for VAX/VMS called Video, from Performance Software. The subtitle says, "...system managers and training coordinators can keep an eye on user activity". Among other things, this package allows anyone with appropriate privileges to see what anyone else is typing and receiving on their terminal (passwords excepted, I suspect), or to "take over" another terminal and broadcast their own commands to it. You can also record terminal sessions and play them back at leisure.

"With the Video Seer utility, system managers can monitor terminal sessions to detect system abuse or simply to identify performance drains on their systems."

Oh joy.

[Funny aside: I just received a computer-printed letter for \_Time\_ Sweepstakes. The first paragraph reads: "... Isn't it time you get that dream house for you and your family in Burbank? Isn't it time you started driving home to Box 6867 in that Mercedes-Benz you've had your eye on for years?..." Don't they know it's hard enough to fit myself into Box 6867, let alone park a Mercedes there?]

Peter Scott (pjs@grouch.jpl.nasa.gov)

## ✓ Power failure problems (RISKS 8.28)

Jonathan I. Kamens <jik@Athena.MIT.EDU> Mon, 20 Feb 89 04:57:16 EST

In <u>RISKS DIGEST 8.28</u>, John Sinteur writes of his previous employers' problems when the power went out and their magnetic card readers failed to work.

About nine days ago, a large part of Cambridge, including the entire MIT campus, lost power for several hours as a result of a gas explosion in a manhole. One result of this was that all of Project Athena (The MIT undergraduate computer system/research project) lost power, including all of the workstation clusters.

The workstation clusters are all accessed by typing a combination into a keypad outside the door of the cluster. However, when the power went out, the keypads all went dead and hence all of the doors could not be opened.

Nevertheless, the people who were sent around to power down all of the workstations (so that when the power came back on things could be brought back up gracefully) were able to get into most (if not all) of the clusters without any trouble. Students leaving the clusters after the power went out realized that the keypads would not open the door, and therefore the last person out of each cluster propped open the door with a garbage can.

I guess it didn't occur to them that this would allow anyone to walk onto campus, walk into a computer cluster and steal every keyboard, mouse and chair in the cluster (The computers themselves are locked down in all but one cluster.).

(Then again, who would want all of those DEC and IBM keyboards and mice? :-)

Jonathan Kamens, MIT Project Athena, jik@Athena.MIT.EDU Office: 617-253-4261

## photographs as evidence (re: digital editing, etc.)

Ernest H. Robl <ehr@uncecs.edu> Mon, 20 Feb 89 14:27:59 EST

Several of the photography trade publications carry regular columns on "forensic photography" -- the making and use of photographs for evidence in civil and criminal cases. The authors of these columns usually stress that photographs themselves are not sufficient for evidence, since such factors as lighting, angle of view (particularly with the use of telephoto or wide angle lenses), etc. can provide a quite different impression from what exists in reality.

When photographs are introduced as evidence, the photographer is called as a witness to testify that the pictures are a true representation of a particular scene, object, etc. The authors of these articles therefore stress the importance of keeping related documentation about when, where, and how the photographs were made, since this can come up during the trial.

Also related to the digital processing of images: There's currently a fair amount of coverage in the photographic trade press about another legal aspect of electronically combined images -- namely who owns the rights to the final product. Since most commercial photographers sell \*rights\* to the use of their images, rather than the physical transparency itself, this can get into a sticky area, since some clients (particularly in advertising) will want

exclusive use of a particular image (and related images) for either a specific time period or for a specific geographic area. The current issue of \_Photomethods\_, a journal for the audio-visual industry, has a questionnaire asking photographers whether they feel digital manipulation of images is a help or poses a threat.

-- Ernest

My opinions are my own and probably not IBM-compatible.--ehr Ernest H. Robl (ehr@ecsvax) (919) 684-6269 w; (919) 286-3845 h Systems Specialist (Tandem System Manager), Library Systems, 027 Perkins Library, Duke University, Durham, NC 27706 U.S.A.

# Stanford and rec.humor.funny -- risks in BBoards

<minow%thundr.DEC@decwrl.dec.com>
21 Feb 89 09:36

[Found this on a local bulletin board. Martin Minow]

This is from the February 20, 1989, San Jose Mercury News:

Computer users worry that Stanford set precedent

They say decision to block bulletin board impedes free acces to public information.

By Tom Philp

Computer scientists at Stanford fear the university has entered a never-ending role as a moral regulator of computer bulletin boards by recently blocking access to a list of jokes deemed to serve no "university educational purpose." Many computer users on campus consider bulletin boards to be the libraries of the future - and thus subject to the same free access as Stanford's library system. Instead, Stanford apparently has become the nation's first university to block access to part of the international bulletin network called Usenet, which reaches 250,000 users of computers running the Unix operating system, according to a computer scientist who helped create the network.

To some computer users, Stanford's precedent is troubling. "We get into some very, very touchy issues when system administrators are given the authority to simply get rid of files that they deem inappropriate on publicly available systems," said Gary Chapman, executive director of Computer Professionals for Social Responsibility, a Palo Alto-based organization with 2,500 members. "My personal view is that freedom of speech should apply to computer information."

Ralph Gorin, director of Academic Information Resources at Stanford, disagrees. "I think that it's very clear that one should be either in favor of free speech and all of the ramifications of that or be willing to take the consequences of saying free speech sometimes, and then having to decide when," Gorin said.

Since the jokes ban, more than 100 Stanford computer users, including a leading

researcher in artificial intelligence, have signed a protest petition. And there is some evidence to indicate Stanford officials are looking for a way out of the dilemma they have created.

The joke bulletin board, called "rec.humor.funny," is one of several bulletin boards that discuss controversial topics. Stanford, for example, continues to permit access to bulletin boards that allow students to discuss their use of illegal drugs, sexual techniques and tips on nude beaches. Gorin said he is unaware of those bulletin boards.

The jokes bulletin board came to Stanford officials' attention in December, after a report about it in a Canadian newspaper. The jokes hit a raw nerve with campus officials, who have been plagued by a variety of racist incidents on campus. And so they decided on Jan. 25 to block the jokes from passing through the university's main computer. "At a time when the university is devoting considerable energy to suppress racism, bigotry and other forms of prejudice, why devote computer resources to let some outside person exploit these?" Gorin explained.

The joke that sparked the complaints is this: "A Jew and a Scotsman had dinner in a restaurant. At the end, the Scotsman was heard to say, 'I'll pay.' The next day there was a newspaper headline, 'Jewish Ventriloquist Murdered." Most of the jokes are not racist or sexist, Gorin said; they are just plain silly or political. An example: "What did Mickey Mouse get for Christmas? A Dan Quayle watch."

But Stanford officials were troubled because the jokes bulletin board is "moderated," meaning that one person controls everything that it publishes. The jokes bulletin board "does not in itself provide for discussion of the issues that it raises," Gorin said. The moderator, Brad Templeton of Waterloo, in the Canadian province of Ontario, publishes only jokes. Comments he receives go on a separate bulletin board, called "rec.humor.d." For Stanford, the existence of a comment bulletin board is not enough because people who call up the jokes will not necessarily see the comments.

The problem with "unmoderated" bulletin boards is clutter, according to Eugene Spafford, a computer scientist at Purdue University who is one of the pioneers of Usenet. The network accumulates the equivalent of 4,000 double-spaced, typewritten pages every day, far too many comments for any person to read. "People who use a network as an information resource like a more focused approach," Spafford said. They is why another, unmoderated, bulletin board that has many comments and fewer - but equally offensive - jokes, is far less popular. Stanford does not block transmission of that bulletin board. Templeton's bulletin board is the most popular of the 500 on Usenet. An estimated 20,000 computer users pull up the jokes on their screens every day, Spafford said.

Usenet has its own form of democracy, calling elections to determine whether a new bulletin board should be created, and who - if anyone - should moderate it. Templeton's jokes bulletin board was created by such a vote. Stanford's decision to block access to it "strikes me as hypocritical," Spafford said. "At best, it's someone who doesn't understand the situation who is trying to do something politically correct."

John McCarthy, a Stanford computer science professor and one of the founders of the field of artificial intelligence, has met with university President Donald Kennedy to discuss his opposition to blocking the jokes. "No one of these (bulletin boards) is especially important," McCarthy said. The point is that regulating access to them "is not a business that a university should go into."

Since deciding to block access to the bulletin board, the administration has referred the issue to the steering committee of Stanford's Faculty Senate. The future of the bulletin board may end up in the hands of the professors. "I think that is an entirely appropriate internal process for reaching that decision," Gorin said.

Added McCarthy: "I should say that I am optimistic now that this ban will be corrected. There are some people who think they made a mistake." ...



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 8: Issue 31

# Monday 27 February 1989

# **Contents**

Bank fraud was "easy"

Stephen Page

Men accused of `hacker' crime

Michael C Polinske

Stanford bboard censorship

**Les Earnest** 

John McCarthy

Jerry Hollombe

Computer writing coach / friend

**Rodney Hoffman** 

British Computer Society policy on safety-critical systems

**Martyn Thomas** 

Reach out and spy

gls

Risks of Running a Hotel

**Chuck Weinstock** 

Singing in the Rain

**Kent Borg** 

[RISKS BARFMAIL]

**PGN** 

Info on RISKS (comp.risks)

# 

Stephen Page <sdpage@prg.oxford.ac.uk> Sun, 26 Feb 89 10:03:38 gmt

From The Independent [London], 24 February 1989, p. 2:

"A 17-year-old junior cashier cheated the National Westminster Bank out of 1m pounds in a computer fraud, a court heard yesterday. ...

Judge Helen Palin criticised the bank for lax security and refused to make a compensation order for 15,000 pounds which the bank has not been able to recover.

... After being given access to the bank's computer system he began by paying 10 pounds into his own account. He then paid himself 12,000 in imaginary cheques. Later, he transferred a credit for 984,252 pounds into the account of a friend ... and celebrated by buying 50 bottles of champagne.

... The judge said: "One of the worrying features of this case is that a young man who hasn't long left school is able to work the system in the NatWest bank on a number of occasions without being found out. Indeed, the general chat within the bank seems to be how easy it is to defraud that bank."

This is a good example of what ensues when system designers build weak controls - or perhaps when users fail to implement them? Too often in the IT community I hear security and controls described as dull and uninteresting - anyone who has had the dreary job of producing a risks/controls matrix will sympathise - but it should NEVER be neglected. I'm glad the judge denied the compensation order.

## ✓ Men accused of `hacker' crime

Michael C Polinske <mcp2@csd4.milw.wisc.edu> Mon, 27 Feb 89 10:12:07 CDT

This appeared in Friday, February 24th's Milwaukee Journal

2 MEN ACCUSED OF 'HACKER' CRIME

By James Gribble of the Journal staff.

Vowing to step up efforts to stop computer crime, a Milwaukee County prosecutor has charged two Milwaukee men with fraudulently obtaining free long-distance telephone service.

The felony charges filed Thursday against Alan Carr, 35 and David Kelsey, 26 are the first so-called hacker crimes to be prosecuted by the district attorney's office.

Working independently, using home computers and similar software programs, the men are alleged to have obtained calling card codes for customers of an independent long-distance telephone company, Schneider Communications.

They then used the codes to bill their personal calls to Schneider's customers, according to a criminal complaint prepared by Asst. Dist. Atty. Jon N. Reddin, head of the district attorney's White Collar Crime Unit.

Reddin said the total theft probably was less than \$1,000, but he said the case reflected a growing problem.

"I have the feeling, from our investigation, that there's a lot of people out there doing this," he said. "The only way to stop it is to prosecute them, because this is theft. It's almost like some one stealing your credit card and using it to make purchases."

Schneider Communications was the victim in this case, Reddin said, because the company had to write off the customer billings for which Carr and Kelsey turned out to be responsible.

According to court records and Reddin, the investigation was prompted by a complaint from Schneider Communications.

The company's computer keeps track of all calls that are rejected because of an improper access code. Clients dialing incorrectly would cause 10 to 30 rejected calls a month, but sometime last year the number jumped to 1,000 or 2,000 per month.

Computer printouts showed the unknown parties were repeatedly dialing the computer and changing the access code sequentially, Reddin said. Hundreds of calls at a time were being made in this fashion, and each time the code was changed one digit at a time until a working code was encountered.

Because the company had no way of knowing where the calls were coming from, Wisconsin Bell placed a tracing device on the line, through which the calls were traced to the phone numbers of Carr and Kelsey.

The men were apparently unaware of each other and simply happened to be involved in similar schemes, Reddin said.

Carr is alleged to have used a bootleg computer called "Hacking Construction Set Documentation." Kelsey is alleged to have used a similar bootleg program called "Mickey-Dialer." The programs were seized in raids at the defendant's houses, according to court records.

Reddin acknowledged that technological safeguards can detect such thefts after the fact but not prevent them. What Carr and Kelsey are alleged to have done can be done by any computer buff with the right software and know-how, Reddin said.

The key to deterring computer crime, in Reddin's view, lies in it's prompt reporting to authorities.

"The best way I can think of to do that is by filing a complaint with our office," Reddin said.

## Stanford bboard censorship

Les Earnest <les@gang-of-four.stanford.edu> 25 Feb 89 01:57:48 GMT Public accounts of the Stanford bboard censorship case, including the San Jose Mercury News article that appeared in <u>RISKS 8.30</u>, give the impression that the administration's ban on newsgroup rec.humor.funny has been effective. Nothing could be farther from the truth -- the "banned" jokes continue to be available on all computers where they were available before and are now more widely read than ever before.

Usenet newsgroups are stored on 9 primary distribution machines at Stanford but are accessed via ethernet from hundreds of computers and workstations on campus. Two of these distribution machines were affected by the administration's ban on rec.humor.funny. The rest of the system, which I organized several years ago, still carries all newsgroups.

Since the "ban" began, every message from rec.humor.funny has been cross-posted to another bboard at Stanford (su.etc) that goes to all machines, including those that are supposed to be censored. There has been no move so far by the administration to deal with this "civil disobedience."

Interestingly enough, the bureaucrats who decided to ban rec.humor.funny didn't have the technical expertise to carry out their intentions, so they came to the Computer Science Department for help. This help was provided even though the individual involved disagreed with what they were doing.

The Usenet primary feed for Stanford is under the control of the Computer Science Department. There was a plan to turn control over to the administration but that plan has now been shelved. The Computer Science faculty voted this week to oppose newsgroup censorship.

Stanford's President Kennedy, who approved the original censorship decision, is now carefully dancing around the issue and has agreed that the Faculty Senate should review and decide on what the University's policy should be. It appears likely that the Senate will agree with the Computer Science Department.

Les Earnest Phone: 415 723-9729

Internet: Les@Sail.Stanford.edu USMail: Computer Science Dept. UUCP: . . . decwrl!Sail.Stanford.edu!Les Stanford, CA 94305

## Stanford bboard censorship

<John McCarthy <JMC@SAIL.Stanford.EDU> [via <LES@SAIL.Stanford.EDU>]>
26 Feb 89 1343 PST

The following statement was passed unanimously at a meeting of the Computer Science Department faculty on Tuesday, Feb 21, 1989.

Statement of Protest about the AIR Censorship of rec.humor.funny.

Computer scientists and computer users have been involved in making

information resources widely available since the 1960s. Such resources are analogous to libraries. The newsgroups available on various networks are the computer analog of magazines and partial prototypes of future universal computer libraries. These libraries will make available the information resources of the whole world to anyone's terminal or personal computer.

Therefore, the criteria for including newsgroups in computer systems or removing them should be identical to those for including books in or removing books from libraries. For this reason, and since the resource requirements for keeping newsgroups available are very small, we consider it contrary to the function of a university to censor the presence of newsgroups in University computers. We regard it as analogous to removing a book from the library. To be able to read anything subject only to cost limitations is an essential part of academic freedom. Censorship is not an appropriate tool for preventing or dealing with offensive behavior.

We therefore think that AIR and SDC should rescind the purge of rec.humor.funny. The Computer Science Department has also decided not to censor Department Computers.

# ✓ Censorship (Re: RISKS-8.30)

The Polymath <hollombe@ttidca.tti.com> 27 Feb 89 23:48:37 GMT

This is the same silly, emotional argument raised every time some form of public or semi-public media refuses to carry someone's pet hobby horse. If you throw out all the emotional baggage about "freedom of speech" and "censorship", Stanford's decision not to carry rec.humor.funny is no more illegal, unconstitutional or censorious then their (de facto) decision not to sell hard-core pornography in the Student's Store.

Only governments can commit censorship, by prohibiting all access to a set of facts. Rec.humor.funny still exists and is still accessible. Those at Stanford who wish to continue accessing it will simply have to sign up with a public access Unix site. (I believe the WELL is conveniently close, as are one or two free-access sites). Stanford is well within it's rights to refuse to spend campus resources to support it.

The Polymath (aka: Jerry Hollombe, hollombe@ttidca.tti.com) Citicorp(+)TTI 3100 Ocean Park Blvd. (213) 452-9191, x2483 Santa Monica, CA 90405 {csun|philabs|psivax}!ttidca!hollombe

# Computer writing coach / friend

Rodney Hoffman <Hoffman.ElSegundo@Xerox.com> 26 Feb 89 14:07:56 PST (Sunday)

From the "Bits and Bytes" page in 'Business Week' 6 March 89:

A PROGRAM SWITCHES FROM THERAPIST TO WRITING COACH

Sometimes talking over a subject with a friend can help you sort out your thoughts before you write a speech or business presentation. A Carrollton (Tex.) company called Xpercom now offers a computer-based "friend" for just that purpose -- a program called Thoughtline that runs on IBM personal computers and clones. It's based on Joseph Weizenbaum's famous Eliza program, written in the early 1960s at MIT. Named after the character in 'My Fair Lady,' Eliza could mimic the conversational skills of a psychotherapist so convincingly that many people believed it actually understood them as a human would and shared with it intimate details of their lives. [See RISKS 8.17 and 8.18] A shocked Weizenbaum ended up writing 'Computer Power and Human Reason,' a leading book on man's relationship to the computer.

Thoughtline, selling for \$295, works a lot like that. It engages authors in written conversations about what they want to say, asking questions based on a script that it constantly adapts as each discussion progresses. It then spits out an outline based on what it has been told. Just like its predecessor Eliza, though, Thoughtline "understands" nothing at all.

## British Computer Society policy on safety-critical systems

Martyn Thomas <mct@praxis.UUCP> Thu, 23 Feb 89 16:34:20 BST

The BCS recently issued the following policy statement on safety-related computer systems (SRCS) in an attempt to raise awareness of the special problems created by programmable systems in safety-related applications. The policy attempts to steer a responsible course between the need to alert society to the increasing risks from poorly-developed SRCS, and the need to avoid creating irrational panic.

We would welcome constructive criticism of this policy from Risks readers.

[declaration of interest: I chair the BCS safety-critical systems group, and wrote the policy statement. It was reviewed and amended by my colleagues in the group before being approved as BCS policy by the Vice-President (Professional), on behalf of the Professional Board.]

The complete text of the policy statement is given below.

THE BRITISH COMPUTER SOCIETY, 13 Mansfield Street, London W1M 0BP

**BCS SAFETY CRITICAL SYSTEMS GROUP** 

Policy Statement on Safety-Related Computer Systems

**PREAMBLE** 

Safety-Related Computer Systems (SRCS) are defined as those systems which, if they go wrong, can lead directly to physical injury of humans.

In almost every case, the potential for injury lies in the system which the SRCS is controlling or monitoring. Assuring the safety of the total system therefore involves several branches of engineering, depending on the application. Most industries are justifiably proud of their safety records.

#### **POLICY**

- 1 Computer systems, appropriately developed and deployed, can enhance the safety of many processes and products, and bring other economic benefits.
- 2 The safety of a system is a system-wide issue, and the safety of a SRCS cannot usefully be considered in isolation from the total system of which it forms part.
- 3 Safety is a relative term; system safety can always be improved at increase cost. The developer therefore has to identify the level of adequate safety and to develop all the subsystems so that this level is achieved overall.
- 4 The probability of error in a system increases with increasing complexity. SRCS should be designed so that their complexity is kept to a minimum, and so that they are isolated from interference from non safety-related subsystems.
- 5 SRCS should be developed and supported by suitably-qualified staff.
- 6 The quality of every SRCS should be the responsibility of a named engineer within an accredited organisation who has up to date training and certification in the relevant technologies.
- 7 Wherever possible, the methods used for developing, supporting and assessing SRCS should be based on sound, scientific and mathematical principles.
- 8 There is urgent need for harmonisation of development standards for SRCS between industries and internationally. The BCS will work with the relevant authorities to achieve this harmonisation.
- 9 The science and technology necessary to achieve and assess highly reliable computer systems is not yet fully developed, and research and development are therefore urgently needed. The BCS calls upon the DTI and SERC to encourage and support the necessary work.
- 10 In view of the limited experience with SRCS, the wide variation in development methods, and the rapid growth in their use, the BCS calls for a system of registration of SRCS, with mandatory fault reporting, so that minimum standards can be enforced and data can be gathered which will allow the success of different approaches to be assessed.
- 11 The BCS wishes to emphasise that there is no evidence that current SRCS pose a serious threat to the public. There is therefore no cause for alarm, although action is urgently recommended on the points listed above.

Martyn Thomas, Chairman, BCS Safety Critical Systems Group

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK. Tel: +44-225-444700. Email: ...!uunet!mcvax!ukc!praxis!mct

# Reach out and spy

<odyssey!gls@att.att.com>
Sun, 26 Feb 11:15:09 1989

The VAX/VMS "spying" package that Peter Scott describes in Risks Digest 8.30 has an old precedent. Aiken C. C. got a Scientific Data Systems "Sigma" time-sharing system around 1969, with terminals in several locations on the Harvard campus. A few months after it was installed I wrote an interactive program called RADIO that monitored any other terminal in the system.

RADIO required no privilege, because the pages of system space that were mapped into user memory included the terminal buffers for the whole system! RADIO made a mockery of confidentiality, and since you could use it to monitor a login sequence, it also made a mockery of authentication. Incidentally, there was no source code for RADIO. Access to the assembler was restricted (as a security feature), so I wrote the program in machine language using the debugger.

The staff at Aiken \_eventually\_ succeeded in destroying all copies of RADIO ... but not without reluctance. They had meanwhile learned the RADIO users' practice of using two RADIOs to talk to each other. If the facility of "talking" seems useful now, it seemed miraculous then. In those days computer system engineers were careful to leave out any kind of "talking" facility for fear of subjecting their systems to FCC regulations.

So far as I know, the only harm that RADIO did was to explode password security. If not for that it might have lived for years.

### Risks of Running a Hotel

Chuck Weinstock <weinstoc@SEI.CMU.EDU> Mon, 27 Feb 89 09:55:33 EST

Those of you who have been ripped off by the alternative operator services (AOS) that provide long distance telephone services to many hotels will be interested in an article that appeared in Friday's Wall Street Journal. It seems that most hotels are neither equipped to bill 976 or 900 calls properly nor to block them. As more and more people discover this, the hotels are finding they are getting interesting phone bills at the end of the month!

# Singing in the Rain

Kent Borg <kent@lloyd.UUCP> Fri, 24 Feb 89 15:07:03 EST Not only have our eyes been the victims of trickery for years (Fred dancing on the ceiling), but so have our ears: In the famous Singing in the Rain dance scene we saw Gene Kelly get rather wet, but we were hearing Gwen Verden (sp?) doing the tapping on the sound track (would that be foot syncing?).

(Ever notice how very well lit the 'rain' drops were in that scene? In real life you often have to put your hand out to find out whether it is raining, in the movies you can always \*SEE\* the rain.)

Hollywood has been using pictures and recordings to 'lie' for years. As a famous camera man once said: "There is nothing natural about natural lighting." The digital doctoring of photos is, in many ways, nothing new, just more powerful.

Kent Borg

P.S. Deception has a long history: "But I \*WATCHED\* him saw her in two!!"

# **✓** [RISKS BARFMAIL]

<The Mailer Daemon <Mailer@KL.SRI.COM> [via PGN]> Mon, 27 Feb 89 12:30:19 PST

[THIS HAS BEEN GOING ON FOR WEEKS NOW. NO ONE HAS COMPLAINED. IS THE NET GOING TO HELL? ARE THESE RISKS READERS FINDING OTHER SOURCES? I AM GIVING UP ON THESE ADDRESSES. PLEASE NOTIFY YOUR FRIENDS. I GOT 400,000 characters in barf mail over the weekend. PGN]

Message undelivered after 3 days -- will try for another 2 days:

- ...@VAXA.ISI.EDU: Cannot connect to host
- ...@III-crg.llnl.gov.#Internet: Cannot connect to host
- ...@EWD.DREO.DND.CA: Cannot connect to host
- ...@LA.TIS.COM.#Internet: Cannot connect to host
- ...@mitre.arpa: Cannot connect to host
- ...@xx.drea.dnd.ca: Cannot connect to host
- ...@red.ipsa.dnd.ca: Cannot connect to host
- ...@sealion.gcy.nytel.com: Cannot connect to host
- ...@wr-hits.arpa: Cannot connect to host
- ...@afsc-bmo.af.mil: Cannot connect to host
- ...@epsilon.jpl.nasa.gov: Cannot connect to host

risks-p@brl.arpa: 550 (USER) Unknown user name in "risks-p@brl.arpa"

AND THEN I GOT EIGHT COPIES OF THE ENTIRE RISKS MAILING BACK FROM Return-Path: <MAILER-DAEMON@cos1.fac.ford.com> 554 mailer mail died with signal 4

THIS IS GETTING MORE AND MORE RIDICULOUS!









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 8: Issue 32

# Wednesday 1 March 1989

# Contents

RISKS-LIST: On Risks of Running RISKS

Gripen prototype crash

**Dave Newkirk** 

Kenneth R. Jongsma

Karl Lehenbauer

A pilot's account of a multi-engine failure

Karl Lehenbauer

Knowing probability just doesn't make a difference

Sumit Dongre

A new ATM risk: bureaucracy

Laura Halliday

IBM's claims for error-free code

Robert Lee Wilson Jr

Re: discussion of computer viruses

**Brent Laminack** 

Re: [RISKS BARFMAIL]

Robert J. Reschly Jr.

Info on RISKS (comp.risks)

# ✓ RISKS-LIST: On Risks of Running RISKS

<Neumann@csl.sri.com>

Tue, 28 Feb 89 13:39:49 PST

Someone answered mail from RISKS, sending directly to RISKS-LIST@KL.SRI.COM! Someone else answered that. It turns out that my macros failed to complete properly, and consequently a window of vulnerability that permits direct rebroadcast (because of a TOPS-20 glitch in handling very large lists) remained open. I have tried very hard to keep this window narrow, and all other attempts get indirected to me personally -- so I know if anyone is trying to hit the window. I've been lucky -- since August 1985, someone hit the direct rebroadcast only once before. And I have not advertisedd the fact that you should not mail to RISKS-LIST, because I thought that might invite some

nastiness from people who resent moderation. (Remember, extremism in the nondefense of moderation is not a virtue.) But very soon RISKS will move to another system, and that window of vulnerability will go away -- only to be replaced by new windows. So, at any rate, apologies for the confusion, thanks to those of you who sent me mail on the subject. Soon we may be onward to lower-risk RISKS.

# ★ Re: Gripen prototype crash (RISKS-8.20)

<dcn@hercules.UUCP>
Fri, 10 Feb 89 07:44:39 PST

I believe the explanation of the recent crash of a Swedish fighter prototype may be less interesting than the last article implied. The pilot was flying the Gripen for his first time, and held the nose too high upon landing. The result was exactly as described before - a wobbly landing that caused a wingtip to hit the runway at about 80 mph. The plane was damaged and the pilot survived. Keep an eye on Aviation Week magazine for a full report.

# Gripen Crash Blamed on Software

Dave Newkirk, att!ihlpm!dcn

<Kenneth\_R\_Jongsma@cup.portal.com>
Tue, 28-Feb-89 06:33:51 PST

In a short article in this week's Aviation Week, the following statements were made:

Saab Blames Gripen Crash on Software

The cause of the accident that destroyed the first prototype of the Swedish JAS-39 Gripen Multirole combat aircraft has been traced to a software problem, program officials said last week.

The pilot, Saab-Scania Lars Radestrom, and the aircraft structure and subsystems have been cleared of fault based on data developed so far.

"We consider the problem to be associated with the control software only," one official said.

No addutional details were given.

# Saab blames Gripen crash on software

Karl Lehenbauer <karl%sugar@uunet.UU.NET> 1 Mar 89 04:20:00 GMT

According to a brief article in Aviation Week and Space Technology (February 27, 1989, page 31), the accident that destroyed the prototype of Sweden's

JAS-39 Gripen multirole combat aircraft was caused by a software problem, according to program officials at Saab.

The article doesn't go into any further detail, other than to say that Saab officials are working on a revision of the Gripen's flight test program to complete flight testing with the remaining four prototypes and still meet their delivery date, which seems extremely optimistic as it is doubtful they have already determined all the rework that will be required to fix the problems that caused the crash, including (it appears) the need for a lot more software QA.

# A pilot's account of a multi-engine failure

Karl Lehenbauer <karl%sugar@uunet.UU.NET> 28 Feb 89 05:40:07 GMT

Although I RISK becoming known as an "Aviation Week" funnel, the following letter to the editor (AW&ST January 30, 1989, pg. 88), quoted without permission, gives a pilot's account of a flight with a multi-engine failure, which I think may be of interest to RISKS readers:

Listening to the news reports on the tragic British Midland crash in the U.K., I was struck by the seemingly unanimous conclusions of the aviation gurus concerning the near impossibility of a two-engine failure of the Boeing 737 using the CMF56 engines.

If the odds on that are improbable, then the flight I had June 14, 1983, was even more so. I was flying as captain for Transamerica Airlines on a DC-8/73, newly reengined with the Snecma/GE CMF56s, and had three engines fail on me simultaneously during a military passenger flight from Kadena AB, Okinawa, to Clark AB in the Philippines.

I was able to airstart the engines during descent and made a successful landing at Clark. Upon taxi-in the engines again failed, and the fourth engine failed as I was parking.

It was later determined that the probable cause was the specific gravity adjustment on the main engine fuel control/MEC was set improperly for the JP 4 fuel being used.

My experience certainly shows that aircraft don't listen to the odds of probability and that, unfortunately, Murphy's Law is always operative.

Don Orlando, Concord, CA

I'm surprised they wouldn't shut down the engines immediately after landing, rather than trying to taxi in, as a precaution, but I have no portfolio in these matters.

Karl Lehenbauer

Knowing probability just doesn't make a difference (Re: RISKS-8.31)

Sumit Dongre <dongre@optilink.UUCP> 28 Feb 89 18:46:19 GMT

This is for all you probabilitists (no, it's probably not a word) out there counting engines on aircraft everytime you get on board.....give it up!!!!

from Aviation Week And Space Techlonlgy: Feb 20, 1989 issue pg 13. quoted without consent and not for profit...so sue me for nothin'.

"BIRD STIKES CONTINUE to be a cause of aviation accidents worldwide... ... Ethopian Airlines experienced some of the most trouble last year. In September, an Ethopian Boeing 737 crash killed 31 people after the aircraft hit birds and damaged both engines during a takeoff from Bahar Dar, Ethopia. Earlier in the year an eagle penetrated the cockpit of an Ethopian 727, breaking the copilot's leg and damaging flight controls. The aircraft made a safe emergency landing in Khartoum, Sudan."

#### Conclusion:

probability burdens our society(ies) needlessly. I'll PROBABLY burn in hell for saying that.

## A new ATM risk: bureaucracy

<laura\_halliday@mtsg.ubc.ca> Tue, 28 Feb 89 15:49:22 PST

Yet another ATM risk...in preparation for a brief holiday in Los Angeles, I elected to change a modest amount of money ahead of time, and use ATMs for more money as I needed it.

The U.S. immigration people didn't like this, and I came very close to having to scrap my holiday. They insist that visitors be able to prove that they can support themselves while in the U.S. (a reasonable requirement), and my bank card wasn't adequate proof (to them) that I could. They grudgingly let me in to the U.S. after asking pointed questions about who I was staying with, who she worked for and how much she made. They flatly insisted that my card meant nothing to them, even when I offered to go to the nearest ATM (50m away), do a balance inquiry and show them the results. I could understand them being concerned about me losing my card (a Risk in its own right). But that wasn't what was bothering them...they were bothered by somebody supporting herself with technology whose implications they obviously didn't appreciate.

- laura

## ✓ IBM's claims for error-free code

Robert Lee Wilson Jr <bobw@ford-wdl44> Tue, 28 Feb 89 16:20:44 PST

The 15 Feb 89 issue of DATAMATION has an article titled "Is Error-Free

Software Achievable?" which praises the Space Shuttle software. (The article would have one believe that the computing systems on the Space Shuttle, both hardware and software, are entirely to be credited to IBM. How does Big Blue always get errors like this to come out in their favor?)

The article quotes Anthony J. Macina of IBM-Houston: "The development of error-free software for these complex real-time systems [national defense, reactor control, air traffic control, and manned space flight] is within the reach of current software development technology." At the beginning of the article that is simplified to:

Is Error-Free Software Achievable?

The answer is yes, says prime NASA contract developer, IBM. And while \$1000 per line of code is prohibitively high for the average IS shop, some valuable lessons can be learned.

Despite this the article says that the 500,000 lines of source code "achieved an "exemplary" error rate of .1 errors per thousand lines of code detected after release." While that is certainly better than usual code, calling the code "error free", when their own data indicate fifty errors, is an interesting metric for quality control!

Bob Wilson, Ford Aerospace Corp., San Jose, CA

# ✓ re: discussion of computer viruses (RISKS-8.31)

Brent Laminack, In Touch Ministries, Atlanta, GA <a href="mailto:cher.uuce-2">brent@itm.uuce-2</a> 28 Feb 89 13:50:26 GMT

Last Sunday's (2/26) comics page had two strips devoted to computer viruses: "Dick Tracy" and "On The Fast Track". One fairly serious about a defense contractor's (Diet Smith) computer, the other humorous about the virus turning all users into clones of the programming manager (Bud Spore). Is comics page where most of the population will get most of its information about viruses?

# Re: [RISKS BARFMAIL]

"Robert J. Reschly Jr." <reschly@BRL.MIL> Tue, 28 Feb 89 22:13:35 EST

Yes, the network is going to hell -- or sinking slowly into the muck. We (BRL) have have been beating on DCA and BBN as we identify particular problems. Only a few other sites/individuals have noticed (and recognised the underlying problems) as near as I can tell. I won't go into details unless you ask for them, but the net result [oof!] is a severe case of routing instability. Networks will come and go at random intervals. We have also seen some breakdown in the Domain Name System as a result of this; which only compounds the difficulty.

As for the specific failure you noted with respect to BRL, our aliases (mail-ID to mailbox mapping) file got trashed late last week. The first 160 or so aliases got deleted. The "postmaster" address also got trashed which was most disconcerting (made it a real bear to tell us about the troubles too!.....)



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 8: Issue 33

# Thursday 2 March 1989

# **Contents**

Viruses and the comics

Jack Holleran

**Hope Munro** 

Hacking in the movies -- Working Girl

**Martin Minow** 

Re: British Computer Society policy statement **Clifford Johnson** 

Hacking and Computer Fraud in the U.K.

**Brian Foster** 

Re: Knowing probability just doesn't make a difference...

**Henry Spencer** 

Reach Out and Spy on Someone

Pete McVay

**Douglas Jones** 

**Emily Lonsford** 

New Sprint Card

Will Martin

US missile-warning radar endangers friendly aircraft

Ken Arnold

Error free code and ancient systems

**Bill Francis** 

Info on RISKS (comp.risks)

### viruses and the comics

Jack Holleran < Holleran @ DOCKMASTER. ARPA> Wed, 1 Mar 89 13:30 EST

In comment to Brent Laminack's observation concerning the discussion of computer viruses (RISKS-8.31) in RISKS-8.32.

- > Is comics page where most of the population will get most of
- > its information about viruses?

If our goals are to make sure the population understands the concept of virus correctly, AND if we perceive that the population reads comics, why not educate some of the cartoonists with the correct perceptions and give them some ideas.

If a person understands the concept, does it matter that the principle was learned from school or the comic strips?

Jack Holleran

(Disclaimer: My opinions only!)

### viruses and comics

<Hope.Munro@mac.Dartmouth.EDU>
01 Mar 89 21:08:10

>Is comics page where most of the population will get most of its information >about viruses?

Apparently so! I clipped a strip out a few weeks ago which was an installment of Bloom County. It depicts Oliver coughing and wheezing, with a head swollen to resemble his Banana 6000 terminal. Then he remarks "computer virus". End of panel. Has anyone seen any other examples of viruses in the comic pages? A possible topic for the next issue of Detective Comics? Let's see the Dark Knight battle these dastardly villians!

- Hone

Hope.Munro@mac.dartmouth.edu

# Hacking in the movies -- Working Girl

Repent! Godot is coming soon! Repent! <minow%thundr.DEC@decwrl.dec.com> 2 Mar 89 08:26

The current (and quite popular) movie "Working Girl" shows two instances of unethical access to computers, both by the heroine, and both praised:

- -- after being put-upon by her boss, she turns to her terminal and pounds briefly on the keyboard. Immediately, the stock-ticker display that circles the room shows a message describing, in somewhat negative and explicit terms, his ability to perform sexually.
- -- subsequently, she accesses the "personal and confidential" files of her new manager's home computer.

Of course, the bosses are nasty, evil creatures and she is the beautiful heroine who marries the handsome prince; so they deserve what they get.

Martin Minow

# ★ Re: British Computer Society policy statement

"Clifford Johnson" <GA.CJJ@Forsythe.Stanford.EDU> Thu, 2 Mar 89 11:11:55 PST

- > From: Martyn Thomas <mct@praxis.UUCP>
- > The BCS recently issued the following policy statement...
- > We would welcome constructive criticism of this policy ...

>

- > 11 The BCS wishes to emphasise that there is no evidence that
- > current SRCS pose a serious threat to the public. There is
- > therefore no cause for alarm, ...

I suggest replacing point 11 with:

11 The BCS wishes to emphasise that there is some evidence that current SRCS pose a serious, growing threat to the public. There is therefore some cause for alarm, ...

In other words, I think the policy statement seriously errs in steering its course of responsibility with a \*political\* caution that in the present social/military context is unfortunately irresponsible. I think public panic is a negligible (but might in any case be a beneficial) risk. Everybody knows that the world's ecology is headed for disaster at rapid rate, but it's difficult to get anyone to care enough even to inform themselves further, let alone to vote to reverse it, let alone to panic.

I think it's not responsible to announce there's "NO evidence" of dangers. Planes fall out of the sky; in medicine, brains are accidentally fried; the innocent are jailed; etc.; because of software bugs. Meanwhile, back at the ranch, a thousand multi-warheaded ICBMs are poised on a computerized hair-trigger, ready for instant launch on receipt of a brief, encrypted launch instruction. If those who are supposed to sound alarms say there's no evidence warranting alarm, who will listen closely to the accompanying advice? If an alarm is sounded, some people may listen, but panic is most improbable. In my opinion, the public needs to be woken up pretty badly.

Could it be that the BCS statement is diercted at management and industrialists, who would be "turned off" by forthright criticism that threatens an uncomfortable degree of change, rather than at the public, who would welcome frankness?

## Hacking and Computer Fraud in the U.K.

<br/>

Outlaw Computer Hacking -- CBI
Peter Large, Technology Editor
(1 March 1989 Guardian newspaper)

Computer hacking should be made a criminal offence, the CBI said yesterday.

The employer's organisation said it was vital to secure a stable base for

computer development, since computers played a major part in the nation's economic competitiveness and "social well-being". Computer buffs were increasingly gaining unauthorised access to confidential information held by banks and other companies in computer databanks, it said.

Much computer fraud is hidden by firms, but the conservative consensus estimate is that the cost to British business is at least #30 million a year.

But computer disasters, caused by software failures, fire and power failures, are reckoned to be cost about ten times that.

The CBI, in its response to the Law Commission's paper on computer misuse, made six proposals:

- \* Hacking cases should be tried by jury;
- \* The concept of "criminal damage" should cover computer programs and data and attacks by computer viruses (rogue programs that can disrupt or destroy data);
- \* Laws should be harmonised internationally so that hackers cannot operate across country boundaries;
- \* The offence of obtaining unauthorised access should include non-physical access, such as computer eavesdropping;
- \* Even unsuccessful attempts to hack should be subject to criminal sanctions;
- \* The value of confidential commercial information should be protected by civil remedies for loss or damage caused by hackers.

The US, Canada, Sweden, and France have outlawed hacking, but it is not an offence in Britain unless damage is done, such as fraud or theft. Last week the Jack Report on banking law proposed outlawing the hacker. The Law Commission has produced a discussion document and is to make firm proposals later this year.

Brian Foster, The Santa Cruz Operation, Ltd., London

# ★ Re: Knowing probability just doesn't make a difference...

<henry@utzoo.UUCP>
Thu, 2 Mar 89 13:20:33 -0500

>"... earlier in the year an eagle penetrated the cockpit of an ethopian >727, breaking the copilot's leg and damaging flight controls...."

it's worth remembering, also, that there's always an unknown risk lurking around a corner somewhere. a few months ago, a 747 diverted to gander after something hit the nose radome and mashed it in, disabling the weather radar. this was first thought to be a simple birdstrike, albeit a rather large bird (possibly a goose:-)). the trouble is, it happened at 33,000 feet! in the absence of major mountains nearby, that is an \*extremely\* high altitude for any

bird, especially a big one. flight international's most recent yearly summary of commercial flight accidents gives the explanation for that one as "hit unknown object at 33,000 ft.".

Henry Spencer at U of Toronto Zoology

## Comment: Reach Out and Spy on Someone

Pete McVay, VRO3-2/E8, 273-5339 <mcvay%tnt.DEC@decwrl.dec.com> 2 Mar 89 07:24

Back in the days when terminals were hardwired to mainframes and VMS was very new, I was a part-time system manager for a VAX/VMS in a course development group. I needed to know critical information at times, such as what programs and task were being run, so I could tell if it was safe to reboot the system or perform other nasty system-management-type tasks. I wrote an enhancement to the "SHOW USERS" command which included the user name, image being executed, amount of logon time, location of the terminal, and other useful tidbits. By running this program I could find out what jobs were being done by whom, and give them phone calls if necessary to see if it was okay to tune the system.

Some users quickly discovered that the program was useful for spying on each other. Two (of about thirty) users were using the program to see what images were being run, and were reporting users to management by name, claiming they were abusing the system and hogging valuable resources. Games were a favorite target, but major file copy operations and MAIL readings also came under attack.

My philosophy was (and is) that users are generally responsible persons and should be consulted in all system policies. I was also chagrined that my "innocent" program was now a major police tool. I removed my program from the system and deleted all sources. Unfortunately, backups were religiously done; these two users convinced management that the program was necessary, so it was restored. I resigned my system management duties in protest. The consequence was a continuing war on the system, with users hiding the names (or images) they were running and the new system manager continually trying to ferret out subterfuge, with stiffer and stiffer penalties...but that is past the scope of this note.

Seeing these new spy programs raises the old issues for me. I can see their benign intent and usefulness. Unfortunately, like guns, they become dangerous and abusive in the wrong hands.

# Reach out and spy

Douglas Jones <jones@herky.cs.uiowa.edu> Tue, 28 Feb 89 11:25:29 CST

We in the computer field forget our past extremely quickly. The Sunday, 26 Feb comments of odyssey!gls@att.att.com about the RADIO program on the SDS Sigma system at Harvard illustrate this, but there are even earlier illustrations.

I used Com-Share's version of the Berkeley Timesharing System on the SDS 940

back in 1968. This had a talk/monitor facility that was used by Com-Share's consultants for on-line user assistance. As highschool students, we weren't allowed to use it, but I saw our teacher use it once.

In 1973, the University of Illinois had a talk/monitor mechanism on their PLATO system. This was a Computer Based Instruction system, and the instructor of a course was expected to be able to monitor any students under their charge. When the system was used outside the instructional context, the "reach out and spy" potential was very real. The developers of PLATO were careful to make talk/monitor use between peers secure -- only after two users had established a conversation through talk could one let the other monitor his or her screen.

Both the Com-Share and Plato systems had nation-wide user communities, and unlike oddyssey!gls@att.att.com, I don't remember any concern about FCC regulations limiting the use of talk facilities.

# Reach out and spy on someone

Emily Lonsford <m19940@mwvm.mitre.org> Tuesday, 28 Feb 1989 10:31:50 EST

There are other products that allow the 'monitor' to watch what the terminal operator is doing - notably CVIEW on VM and a product by Clyde Digital Systems on the VAX. CVIEW at least has an internal ID/password scheme, which of course should be enabled. And it gives a warning message to the person being watched but it's not clear enough for the novice "spy-ee."

I once worked for a utility company that had a couple of hundred customer service operators (using 2260 terminals...it was a long time ago!) and their supervisors could listen in on their phone conversations to make sure that they were doing their jobs and being polite, etc. The operators could also signal for assistance if the customer became irate. But the real use was for performance monitoring. Either it was a condition of the job, or it didn't occur to anyone to complain about invasion of privacy, which it surely was. There are a lot of parallels between this and the 'spy' products.

On the other hand, a case could be made that the "owner" of the system has a right to know what it's being used for; for example, no fair using your PC at work to do your resume or run a business on the side.

Clearly there has to be some reasonable middle ground. For myself, if it's so sensitive or private, it's encrypted or on a floppy and locked away.

\* EMILY H. LONSFORD, MITRE - HOUSTON W123 (713) 333-0922

## New Sprint Card

Will Martin -- AMXAL-RI <control@ST-LOUIS-EMH2.ARMY.MIL> Wed, 1 Mar 89 14:54:22 CST

The following is from the "Federal Bytes" column on the last page of Federal Computer Week, Feb. 13 '89:

#### **PHONE ID**

US Sprint announced last week at Comnet that it is testing a telephone calling card this is activated only by the card holder's voice.

Fred Lawrence, Sprint's executive vice president for network development, said the Voicecard would work a little like the company's Foncard: Callers dial the phone number printed on the card, adding a second number such as a birthdate, and then give a two-second verbal password. Sprint equipment compares the voice print with one that is on record. The call goes through only if the voice prints match, Lawrence said.

Sprint plans to evaluate its test results this spring to determine whether there is a market for the card.

What isn't clear, of course, is if you go through all this before you can actually begin to dial the number you are trying to call. Maybe this is a way to call an 800 number and then get into a mode so that you can make a series of calls authenticated by the initial voiceprint signon process. It seems a lot of overhead for a single short call. If the card has a magstripe and you run it through a reader on the phone, and then only have to speak your "password" phrase before dialling the number you want to reach, it won't be too bad.

I wonder how easily the user (or a cracker) can change the voice "password" (if at all), and the actual degree of matching that is performed on it. How will noisy environments (airports, etc.) affect the recognition/verification process? Anybody out there participating in this test? Please post your comments and evaluation!

Regards, Will Martin [Will sent this to another list as well. Please respond to HIM and we'll let him collect the responses in an orderly fashion... PGN]

# ✓ US missile-warning radar endangers friendly aircraft (Re: RISKS-8.28)

Ken Arnold <arnold@apollo.com> Sat, 25 Feb 89 19:54:59 EST

Jon Jacky submits:

>ADEFENSE RADAR MUST TURN OFF AS PLANES LAND - AIR FORCE FEARS SYSTEM >COULD TRIGGER A BLAST (no author given)

> ...

>The interruptions are to avoid accidental detonations of tiny explosive >charges found in virtually every military weapons system and in the planes >and ships that deliver them.

Doesn't one wonder what one's enemy could do with this data? Imagine -- all they have to do is build large radar installations, and, at no extra charge, they can cause incoming weapons to blow themselves up (or otherwise interefere with their systems). Once again, the more sophisticated technology is also vulnerable in unexpected ways.

#### Ken Arnold

# Error free code and ancient systems

"Francis,Bill" <RISKS@GRIN1.BITNET> Thu, 2 Mar 89 15:58:31 cdt

In a recent issue of RISKS, Bob Wilson cites a Datamation (Feb 15, 1989, p.53,56) article that reports on "error-free" code developed by IBM for the space shuttle. Bob points out several fallacies of the article, let me add this comment ....

The low error rates cited were achieved largely because the programmers worked on an ancient, and stable, hardware platform (IBM 360)for years and years!

How many programmers have the luxury of such stability in the commercial market and in most of the defense market?

The tradeoffs between error rates and computer power are obvious.

Bill Francis, Noyce Computer Center, Grinnell College, Grinnell, Iowa



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 8: Issue 34

# Thursday 2 March 1989

## **Contents**

- German hackers breaking into LOS ALAMOS, NASA,... Claus Kalle via Mabry Tyson
- The Gumbel Machine Becomes a Candid Camera **PGN**
- (Un)fairness in European s/w protection Herman J. Woltring
- Info on RISKS (comp.risks)

# German hackers breaking into LOS ALAMOS, NASA, ...

Mabry Tyson <TYSON@Warbucks.AI.SRI.COM> Thu, 2 Mar 89 14:55 PST

Date: Thu, 2 Mar 89 10:44 PST

From: A0061%DK0RRZK0.BITNET@cunyvm.cuny.edu

To: INFO-NETS@Think.COM

Subject: hackergerman hackers breaking into LOS ALAMOS, NASA, ...

Three hours ago, a famous german TV-magazine revealed maybe one of the greatest scandals of espionage in computer networks:

They talk about some (three ?) german hackers (West Germany) breaking into several secret data networks (LOS ALAMOS, NASA, some military database,

(Japanese) war industry, and many others...) in the interests of the KGB,

USSR. They got money (sums about 50000-100000\$ are mentioned) and even drugs,

all from the KGB, the head of the politic TV-magazine told.

Read more about it in tomorrow's newpaper....

Many greetings from Cologne	^ ^	
1111		
Claus Kalle		
Cologne University, Regional Con	nputing Center / \/ \	
1 11 1		
BITNET: A0061@DK0RRZK0	1 V 1	
ARPA · A0061%DK0RR7K0 BITNE	T@WISCVM WISC FDII /	١

Letter: Regionales Rechenzentrum der Uni Koeln | The |

Robert-Koch-Str. 10 | Koeln |
D-5000 Koeln 41 | Cathe- |
West Germany | dral |

#### The Gumbel Machine Becomes a Candid Camera

Peter Neumann <neumann@csl.sri.com> Thu, 2 Mar 1989 14:52:50 PST

For those of you who did not notice, NBC's TODAY show Executive Producer Marty Ryan asked Bryant Gumbel for a candid evaluation of the show's on- and off-camera staff, which he wrote on-line. Recently the private report was `apparently stolen out of Gumbel's computer file and then given by an NBC employee to a reporter for Newsday." There were lots of red faces. (Source: San Francisco Chronicle article by Jay Sharbutt of the LA Times, 1 March 1989, p. E1.)

# ✓ (Un)fairness in European s/w protection

<WWTMHJW@HEITUE5.BITNET> Tue, 28 Feb 89 13:22 N

#### A DRAFT PROPOSAL ON SOFTWARE PROTECTION FOR THE EUROPEAN COMMUNITY

A few weeks ago, the Council of the European Communities in Brussels/Belgium published a draft "Proposal for a Council Directive on the Legal Protection of Computer Programs" [COM(88)816 (not final)], written by Lord Cockfield M.P. in agreement with Mr Narjes and Mr Sutherland. Until January 1989, Lord Cockfield (pronounced as "cowfield") was Council Commissioner for the Internal Market in the Community. As the document seems to challenge various copyright/author's right doctrines in the Member States of the Community, it is likely to elicit considerable debate.

From a Risks and Anglo-American law point of view, the draft evokes a number of questions to be discussed below. These concern (a) the Anglo-Saxon Law concept of "Fair Dealing" which is more restricted than its "Fair Use" counterpart under section 107 of the US Copyright Act (for example, wholesale copying for classroom use is not allowed), (b) copyright/"author's right" in the case of commissioned works or works created by virtue of employment, and (c) the scope of protectability in the form/contents or expression/idea dichotomy under classical copyright which is largely responsible for the software "look and feel" controversy in the USA.

#### (a) Fair Dealing

The draft proposes that "computer programs" (also to include source code and documentation from which the program could be written) should be treated like any other literary work under the Berne and Universal Copyright Conventions, including the standard exemptions for literary works under national legislation in the Member States. This definition goes much further than the 1977 defini-

tion of the World Intellectual Property Organization (WIPO) in Geneva which is responsible for administrating the Berne Copyright Convention (the BCC recognizes moral rights and does not require copyright claim formalities on a work). In 1985, a joint WIPO/UNESCO meeting on Software Protection refused to include source code in the definition of "computer programs".

The most important states of the European Community are Western Germany, France, and Great Britain. Following copyright law revisions in France (1985), Western Germany (1985), and Great Britain (1988), copyright exemptions are quite different between these countries. In Germany, unauthorized copying for scientific purposes is standard for literary works (not too much, though), but "programs for data processing" cannot be copied without authorization. In France, all USE and copying of "software" (including documentation) is controlled, except for the making of a single back-up copy. In Great Britain, the classical "Fair Dealing" exemption for research and private study, review, criticism, and news reporting was maintained last year for commercial research, despite "immense pressure from monopolistic concerns that wish to restrict information" (E. Nicholson M.P., debate on the Copyright, Designs and Patents Bill, 19 May 1988); the same has recently happened in Canada. In both countries, computer programs are to be treated like any other literary work.

It may be that the 1985 German and French law revisions were largely motivated by a desire within the software industry to use copyright law for creating trade-secret protection for the pure information or know-how underlying a software package. If decompilation (a form of research through analysis or reverse-engineering) is outlawed, know-how is protected against retrieval from a software package, but independent invention of such know-how and its use for creating another software package remain free. In the European Commission's "Green Paper on Copyright and the Challenge of Technology" published in June 1988, reference was made to a general agreement within the information industry that "independent invention (...) and reverse engineering" should be allowed lest competition would be stultified, and Lord Cockfield's draft proposal seems to ignore the latter part of this citation.

On p. 26 of the draft, reference is made to "(...) the Anglo-Saxon law concept of 'Fair Dealing' by which reproduction of insubstantial parts of literary works is permitted under certain circumstances". In this wording, the differences between German, French, and British law seem insubstantial, since proper research, review, criticism etc. of a computer program will usually require substantial if not complete copying. In the case of object code, this would involve decompilation which under copyright law doctrine is a form of copying/reproduction. In the case of original or decompiled source code, this would involve listing, compilation, and running which are also (interpreted as) legally relevant forms of copying/reproduction.

However, Lord Cockfield's suggestion is incomplete, as the Anglo-Saxon law concept of "Fair Dealing" is not confined to insubstantial copying of a work (whether a book, paper, computer program, or other literary work). Thus, there are considerable differences between major Member States within the Community, with an equal competition opportunity between Silicon Valley (California) and Silicon Glen (Scotland): under Anglo-American Law, continental-european software may be investigated while Anglo-American software cannot currently be investigated in France and Western Germany unless authorized by the copyright holder. This, of cource, constitutes a distinctive competitive advantage out-

side the European continent.

I believe that copying of a complete work, such as a computer program, may be necessary for fair dealing to apply if done for one of the statutory purposes, i.e., for research or private study, review, criticism, or news reporting. In the words of Barry Torno's "Fair Dealing -- The Need for Conceptual Clarity on the Road to Copyright Revision" (Consumer and Corporate Affairs Canada 1981, ISBN 0-662-11746-8, pp. 32 seq.):

"It might very well be the case that, upon proper application of fair dealing considerations, there will be very few situations in which a finding of fair dealing will prevail where an entire work has been taken. However, to preclude such a possibility AB INITIO is to fetter the dynamic nature of fair dealing unnecessarily.

In what is widely regarded as one of the most incisive Commonwealth explorations of fair dealing, Lord Justice Megaw of the British Court of Appeal stated in the 1971 case of Hubbard et al. v. Vosper et al. (1972, 2 Q.B. 84):

'It is then said that the passages which have been taken from these various works ... are so substantial, quantitatively so great in relation to the respective works from which the citations are taken, that they fall outside the scope of 'fair dealing'. To my mind, the question of substantiality is a question of degree. IT MAY WELL BE THAT IT DOES NOT PREVENT THE QUOTATION OF A WORK FROM BEING WITHIN THE FAIR DEALING SUBSECTION EVEN THOUGH THE QUOTATION MAY BE OF EVERY SINGLE WORD OF THE WORK ...'

On 9 Feb 1972, the Appeal Committee of the British House of Lords dismissed a petition for leave to appeal against this verdict. Note that 'fair dealing' does not in a statutory way distinguish between various forms of reproduction such as quoting, listing, or translating; this has been left to case law. Furthermore, computer programs were hardly discussed by Torno.

In "Copyright and the Computer" (Consumer and Corporate Affairs Canada 1982, ISBN 0-662-11748-4), John Palmer and Raymond Resendes from the University of Western Ontario wrote on p. 126:

"Allowing fair dealing provisions for computer software seems questionable. On the one hand, there should be no objection to allowing researchers for PRIVATE (and personal) study and review once the software has been developed and marketed. On the other hand, the loss of a single sale of the software could result in the loss of revenue to the developer of thousands of dollars. If fair dealing provisions are allowed for computer software, they should be limited specifically to personal study and research concerning the SOFTWARE ITSELF, and they should NOT include study and research which uses the software for the study and research of other questions."

In my mind, the latter would not necessarily apply always, as in the case of software published in the academic literature or via non-commercial electronic mail libraries (e.g., NETLIB@RESEARCH.ATT.COM, cf. the paper by Dongarra & Grosse in the May 1987 issue of the Communications of the ACM). Especially numerical software is widely available for non-commercial use, and this aspect seems to have been overlooked by most writers on software protection, even

though such software is not necessarily in the public domain.

A Canadian Library of Parliament report (Monique He'bert, "Copyright Act Reform", ISBN 0-660-12598-6, 1987, p. 5) states:

"(E)ven when substantial reproduction has occurred, users may be exonerated if they come within one of the statutory defenses. The most important of these is the 'fair dealing' provision which excuses 'any fair dealing with any work for the purposes of private study, research, criticism, review, or newspaper summary'."

Wrapping up these quotations in a software context, I think that copying of a complete work such as a computer program may be necessary for FAIR dealing to hold; only in this way, a researcher, reviewer, or criticist may be able to "tell the truth, the whole truth, and nothing but the truth". This applies to profitable situations, where the underlying but unprotected ideas (trade secrets?) of a computer program are to be found and used for creating a different, and hopefully better computer program. Under the US "Fair Use" doctrine, this is perfectly lawful, industrial practice; cf. the "clean room" procedure, where one team analyses a competitor's package, while a second, clean team writes a new package from the first team's specifications. For a hardware product under, e.g., patent law or semiconductor topography protection law, research is perfectly legitimate, and there is no reason why this should be outlawed for software, especially since hardware and software can often be interchanged.

Similar arguments hold for the non-profit situation, as when claims about the quality of a commercial software package in the academic or commercial literature are to be verified by scientists or consumer organisations, or when a software package is suspected of endangering human life, health, or property; this latter aspect was addressed in Risks Digest Vol. 8, No. 5 of 11 Jan 1989 with respect to the Therac-25 radiation therapy machine malfunction.

While the Universal Copyright Convention requires a Copyright notice to be included in a work for copyright protection to hold, such a formality is not required under the Berne Copyright Convention recently ratified by the USA which are currently the world's leading software producer. By consequence, various "fair" forms of copyring are currently under threat of being outlawed even if no copyright claim is provided on a work.

Of course, copying for unfair purposes should be prevented, both in a profitable and non-profitable context. For example, a number of recent, federal US verdicts that the US Copyright Act should yield to the 11th Amendment are reason for serious concern: see "An Open Letter on Piracy", Software Magazine 8(3), March 1988, republished in ACM's Computers & Society 18(3), July 1988. Under the 11th Amendment's grant of sovereign immunity to states, civil suits for copyright damages against state instrumentalities (e.g., state universities!) will be lost before trial.

#### (b) Work for hire

Under the Anglo-American "work for hire" rule, copyright law usually gives all exploitation rights to the employer, and sometimes even to the commissioner of a copyrightable work; moral rights have been excluded for computer programs in

the United Kingdom, and they have been limited in France. In Germany, however, moral rights have been maintained in full, and case law has given an implicit right of use to the employer or commissioner. Such use may involve sales to third parties if this is the (implied) consequence of the contract. Lord Cockfield has proposed that all rights on software created under employment or commission should revert to the employer or commissioner (unless parties agree otherwise), and this will undoubtedly cause considerable disagreement in most Member States of the Community, at least for commissioned software.

Under the continental-european doctrine of "author's rights", certain moral rights (paternity, divulgation, integrity) are inalienable from the natural author(s) who create a work, and it is largely this aspect which underlies the debate within the European Community (moral rights were a strong issue in the USA in the debate around the Berne Convention Ratification Bill). From a Risks point of view, I would think that author's rights and author's duties should be seen in conjunction. With the commercial pressure that deadlines are met in software projects (cf. the Risks Digest issue quoted above), an employed or commissioned author should, in my view, be able to invoke his moral rights in order to offset any pressure from employer or commissioner to deliver on time. While Lord Cockfield mentioned the right of paternity (i.e., the right to be named as the author of a work), it is too simple to leave responsibility for the quality of a work, closely related to the moral rights of divulgation and integrity, with the entity that delivers a software-related product to a customer. If an employed or commissioned author has good reason to believe that his work has been insufficiently tested, his "droit de divulgation" should be used to prevent premature delivery to unsuspecting customers. Personal liability for a defective software package should complement this moral right as a moral obligation.

(c) Ideas or contents v. form or expression under Copyright

Traditionally, copyright protects merely the expression or form of a work, not the "naked ideas", contents, or pure information in the work. The boarderline is a difficult one, as exemplified by Lord Cockfield's proposal on algorithms and on accessability of interfaces which, for scientific progress and compatibility between different manufacturers' products to be possible, should be free to anyone:

Chapter 1, Article 1, "Object of Protection",

•••

3. Protection in accordance with this Directive shall apply to the expression in any form of a computer program but shall not extend to the ideas, principles, logic, algorithms or programming languages underlying the program. Where the specification of interfaces constitutes ideas and principles which underly the program, those ideas and principles are not copyrightable subject matter.

I hope that this posting on the Risks Digest (and perhaps on other lists) will elicit a debate that could be fed back to the European Commission. I look forward to such reactions.

Herman J. Woltring



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 8: Issue 35

# Monday 6 March 1989

# Contents

NASA to replace top-level personnel with Expert Systems

**Dave Davis** 

A Touching Faith in Technology

**Ruaridh Macdonald** 

Computer catches thief

Randall [!] Davis

Computer espionage: 3 `Wily Hackers' arrested

Klaus Brunnstein

Re: West German Hackers

Dana Kiehl

The word "hacking"

**Geoffrey Knauth** 

Rao V. Akella

747 Simulators Can't Simulate Flight 811 Failures

Scot E Wilcoxon

Viruses in the comics

Peter Merel

Tom Parker

Len Levine

**Guy Robinson** 

Info on RISKS (comp.risks)

## NASA to replace top-level personnel with Expert Systems

dave davis <davis@community-chest.mitre.org> Mon, 06 Mar 89 12:52:29 -0500

From the 6 March New York Times, page 1, comes a news item that NASA faces the possibilty of retirement of ALL of its senior and top-level managers, engineers and scientists within five (5!) years.

To address this, NASA plans to continue a trend that it has already been implementing. That is, it will seek to capture expert knowledge via expert systems, and where it can, replace people with embedded systems containing this expertise. Currently, NASA is utilizing such systems to perform Space Shuttle fueling and monitoring, countdown diagnostics (some risks there...), and telemetry monitoring and interpreting. For example, NASA says that it can take two years to train an individual to interpret a data stream from a satellite (after which he/she is probably a bit warped). NASA was able to completely replace the console operator in an example of this with an embedded system which included friendlier user display and interpretive knowledge.

The article points out that not all of those elegible for retirement will take it, however, if this program is successfull, the decision may be made for some of them.

Many of the technical risks of such a program are numerous and obvious. One which may not be quite so obvious is stagnation, that is, how will NASA incorporate new knowledge into its systems and how will such knowledge be developed and recognized. This may be a non-problem, in that previous technological advances (see the steam engine) taught us more than was ever expected when they were invented.

Dave Davis, MITRE Corp., 7525 Colshire Dr, McLean, VA 22102

## A Touching Faith in Technology

MACDONALD@hermes.mod.uk <Ruaridh Macdonald> 6-MAR-1989 12:15:22 GMT

The question of whether we in the U.K. should carry identity cards is currently being debated, particularly in the press. It has been stirred up by the Government's intention to introduce identity cards for attendees at football matches, as part of an attempt to curb hooliganism.

The following appeared as the leading article in The Times on 10th February (reproduced without permission), and shows a touching, if misplaced, faith in technology by non-technologists. (The highlighting is my own.)

"British suspicion of identity cards is deeply rooted. But it is not as profound as is commonly supposed, according to a survey out today.

"Identity cards were compulsory during and immediately after the Second World War. ... 57 per cent of those questioned in today's survey were in favour ...

"... everyone has a unique collection of official numbers, including a health service number, a national insurance number, a passport number, another on their driving licence and one issued by the Inland Revenue. However free and libertarian people might feel, they are deeply enmeshed by 20th century bureaucracy - and for the most part accept their fate without complaint.

"The adoption of an identity card, at least on a voluntary basis, which would carry such numbers - name, date of birth, nationality, signature and perhaps blood group - would surely be an advantage for everybody. In one sense it would be a master key. GIVEN THAT TECHNOLOGY SHOULD MAKE IT IMPOSSIBLE TO FORGE THEM, such cards could quickly establish one's bona fide. . . . ."

#### Ruaridh Macdonald

# Computer catches thief

Sun, 5 Mar 89 15:25:10 est

In Risks 8:31, Michael C Polinske gives us the newspaper story of two men caught stealing long distance telephone service, that ran with the headline:

#### 2 MEN ACCUSED OF 'HACKER' CRIME

Interesting that the theft of service via hacking gets all the attention, when part of the story (reproduced below) makes it clear that the headline could equally well have been:

#### COMPUTER CATCHES TWO STEALING PHONE SERVICE

...

The company's computer keeps track of all calls that are rejected because of an improper access code. Clients dialing incorrectly would cause 10 to 30 rejected calls a month, but sometime last year the number jumped to 1,000 or 2,000 per month.

Computer printouts showed the unknown parties were repeatedly dialing the computer and changing the access code sequentially, Reddin said.

## Computer espionage: 3 'Wily Hackers' arrested

Klaus Brunnstein <br/> <br/> klaus Brunnstein <br/> <br/> / Strunnstein / Strunnstein

Today (February 2nd,1989), 3 hackers have been arrested in Berlin, Hamburg and Hannover, and they are accused of computer espionage for the Soviet KGB. According to TV magazine 'Panorama' (whose journalists have first published the NASA and SPANET hacks), they intruded scientific, military and industry computers and gave passwords, access mechanisms, programs and data to 2 KGB officers; among others, intrusion is reported of the NASA headquarters, the Los Alamos and Fermilab computers, the US Chief of Staffs data bank OPTIMIS, and several more army computers. In Europe, computers of the French-Italian arms manufacturer Thomson, the European Space Agency ESA, the Max Planck Institute for Nuclear Physics in Heidelberg, CERN/GENEVA and the German Electron Accelerator DESY/Hamburg are mentioned. Report says that they earned several 100,000 DM plus drugs (one hacker evidently was drug addict) over about 3 years.

For the German Intelligence authorities, this is `a new quality of espionage'. The top manager said that they had awaited something similar but are nevertheless surprised that it happened so soon and with such broad effects.

Summarizing the different events which have been reported earlier - NASA and SPANET hacks, Clifford Stoll's report of the 'Wily Hacker' - I regard this as

essentially the final outcome of the Wily Hackers story (with probably more than the 3 which have now been imprisoned). It is surprising that the Intelligence authorities needed so long time (after Cliff's CACM report, in May 1988!) to finally arrest and accuse these crackers. Moreover, the rumors according to which design and production plans of a Megabit chip had been stolen from Philips/France computers seems to become justified; this was the background that CCC hacker Steffen Wernery had been arrested, for several months, in Paris without being accused. CAD/CAM programs have also been sold to KBG.

Klaus Brunnstein University of Hamburg/FRG

[There were numerous articles on this topic over the weekend. Because almost every paper had a little something, our coverage here will remain light until we have some more definitive reports. PGN]

#### re: West German Hackers

Dana Kiehl <Kiehl@DOCKMASTER.ARPA> Fri, 3 Mar 89 09:36 EST

Regarding today's (3rd of March) news on the West German Hackers who got money and drugs from the KGB:

If the story is accurate, this brings up another point about hacking: they could be working for the enemy. Some people consider hackers as harmless pranksters or not much of a threat but this story shows that the bugger running around your system may very well be working for your competitor or even the other side. Scary thought

### ★ The word "hacking" (RISKS-8.33)

Geoffrey Knauth < lloyd!sunfs3!geoff@hscfvax.harvard.edu> Fri, 3 Mar 89 10:14:09 EST

I object strongly to Peter Large's use of the words "hacking" and "hacker" in a continually negative context, especially since he proposes to outlaw "hacking."

Much hacking is wonderful for society. Take Richard Stallman, for example, the driving force behind GNU and the Free Software Foundation. He is a dedicated hacker in the best sense of the word, and I only wish I could hack so well. I cannot accept statements which confuse productive hacking with harmful acts.

# ✓ [RISKS] `Hey...Who are you calling a "hacker"?' (RISKS-8.33)

"Rao V. Akella" <CCCSRAO@UMNHSNVE.BITNET> 03/03/89 19:28:42

> Computer hacking should be made a criminal offence, the CBI said yesterday...

Hey, hey, wait a minute...since when has the term "hacker" become synonymous with "criminal"? I strongly object to the insinuation that ALL hackers are criminals. I personally consider the appellation "hacker" to be a badge of honour. I would dearly like to call myself "hacker", but in my own opinion I'm not good enough yet. I would love it if anyone called me a "hacker" (I badly want someone to, but no one has - yet.)

According to Steven Levy's "Hackers", the term "hacker" was coined at MIT in the 1950s, and it implied 'serious respect', 'innovation, style and technical virtuosity' and 'artistry'. Why has this word come to stand for serious wrong-doing today? Today's (March 3rd, 1989) NBC Nightly News with Tom Brokaw had a story about 3 West German "computer hackers" being convicted (and 5 other "hackers" being charged) for providing the Soviets with sensitive computer passwords. Why is it that a computer programmer automatically becomes a "hacker" when it involves a crime? Why couldn't they have reported '...3 West German computer programmers have been convicted...'? If some of you think that I'm making a mountain out of a molehill, then I demand that all programming job classifications be renamed to "Applications Hacker", "Systems Hacker", and so on. It would make at least me very happy. In my humble opinion, this much maligned word is becoming as overused and abused as that other overloaded operator of the late 1980s: "computer virus".

Rao Akella, Research Assistant, University of Minnesota CCCSRAO@UMNHSNVE.BITNET

# **▼ 747 Simulators Can't Simulate Flight 811 Failures**

Scot E Wilcoxon <sewilco@datapg.mn.org>
5 Mar 89 04:00:27 GMT

The Wall Street Journal of March 1 1989, page 1, had an article on United's Flight 811 which mentions:

"The Role of Skill

Training prepares airline pilots for all sorts of emergencies, but nothing like the one Flight 811 encountered. There aren't any simulator programs for losing two engines on the same wing of a 747, let alone flying with a 10-by-25 foot hole in the fuselage."

The wording of "on the same wing" suggests there are simulators which allow one engine on each wing to be lost, so the possibility of multiple engine failure has not been completely overlooked.

The article later points out there is no way to prepare for all the possible things that can go wrong.

Scot E. Wilcoxon sewilco@DataPg.MN.ORG {amdahl|hpda}!bungia!datapg!sewilco Data Progress UNIX masts & rigging +1 612-825-2607 uunet!datapg!sewilco

#### Viruses in the comics

Peter Merel <pete@attila.oz.au>

#### Sun, 5 Mar 89 23:58:16 AES

Viruses and other nefarious hacker activities have been included as plot devices in DC's revival of 'The Shadow'. In this book The Shadow has returned from Shambhalla (sp?) to the West after an absence of over 40 years to carry on his war on the evil that men do. Two of the new agents recruited into his service belong to a hacker consortium calling itself 'The Shadownet'.

While the book is not intended as any sort of explication of hacking activities or computer activities in general, I've not seen any outright mistakes in its presentation of hacking. Of course I'm not sure whether it is really that easy to hack into the Orbital Mind Control Lasers.

Worth a read if you're interested in the RISKS to society of coordinated networks of technically competent people. Also hysterically funny. "The weed of crime bears bitter fruit..."

#### Viruses in the comics

Tom Parker <firewind%xroads%sunburn@sun.UUCP> 3 Mar 89 22:33:25 MST (Fri)

I can think of a few examples of computer virii in the comics. In a semi-recent issue of "Alpha Flight", the story revolves around a virus who's function is to "transfer credits to author". The virus is "written in machine code so it can infect any machine". In a not so recent issue of Iron Man, a "tapeworm" is introduced into the world's computer network to erase certain blueprints where ever they might appear.

In both instances the virii are portrayed as invincible and able to infect any computer. I'm afraid that any depiction of viruses in the comics is going to be simplistic and pretty much out of touch with reality.

Tom

#### Viruses in the comics

"Len Levine" <len@evax.milw.wisc.EDU> Fri, 3 Mar 89 11:27:38 CDT

Kelly, a cartoonist in the San Diego Union posted a cartoon recently with several panels discussing the danger of swapping floppies with comments from the cartoon characters like:

He: I think we should do it. She: No way, I hardly know you.

He: Come on, you only live once.

She: No way, there are too many viruses out there.

He: You know you want to.

She: The threat of infection mortifies me.

He: \_Please\_!

She: Well maybe, just this once.

He: [he hands her a floppy]

She: Trading software is so risky these days.

This is good educational techniques. It gets the point across.

Leonard P. Levine e-mail len@evax.milw.wisc.edu |
Professor, Computer Science Office (414) 229-5170 |
University of Wisconsin-Milwaukee Home (414) 962-4719 |
Milwaukee, WI 53201 U.S.A. Modem (414) 962-6228 |

## Intelligent treatment of viruses in comics

<"Guy\_Robinson.SBDERX<"@Xerox.COM> 6 Mar 89 02:47:04 PST (Monday)

Marvel Comics traditionally deal with computers in a very intelligent way. Very often the younger intelligent "super-heroes" are seen using computers for both work and recreation. This is not to say something totally unfeasible happens from time to time but this simply requires suspension of disbelief.

The example in point I want to use is the current storyline concerning the Vision, an android. Due to a previous severe computer crime the Vision was kidnapped and stripped bare of all software.

To prevent a simple back-up being taken a virus was used to destroy all saved copies of the Vision's personality. This virus propagated itself around several machines to ensure the task was completed.

One problem this situation raised was that the Vision's human WIFE was a little distraught! Could this be a whole new type of RISK to bear in mind?

Guy



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 8: Issue 36

# **Tuesday 7 March 1989**

#### Contents

Malicious Hacking

**Gene Spafford** 

News from the KGB/Wilv Hackers

Klaus Brunnstein

The fight to purify the word "hacker" is lost

Steve Bellovin

**Brad Templeton** 

Dangers of Spy programs

John ffitch

Re: reach out and spy on someone

**Vandenberg** 

Social effects of viruses

**Don Alvarez** 

Previous message to RISKS misunderstood [Power Failure Problems]

John Sinteur

Info on RISKS (comp.risks)

### Malicious Hacking

Gene Spafford <spaf@cs.purdue.edu> 7 Mar 89 19:45:38 GMT

I've recently been in contact with someone doing a study for DOE on malicious hacking. In particular, the following 3 topics have been specifically targetted for attention:

- 1) Have there been any documented cases of loss of life, threat to life, massive economic loss, or other disastrous circumstances caused by someone breaking into or hacking on a system? This is \*not\* concerned with system failures or poor design, but rather with acts of specific intent.
- 2) Have there been any documented (or strongly suspected) cases of hacking/cracking/etc. for purposes of corporate espionage or sabotage, or for service to a foreign government? The recent West German arrests are one case...are there others?

3) Has anyone (other than Sherry Turkle) done any work on the psychological profile of someone likely to break into systems, be a compulsive hacker/cracker, etc? If so, do you have references?

If you have any material on the above, I'd appreciate hearing about it. I'd like to see if for my class on ethics & responsibility, and my contact would like it for his report. I'm sure that anyone contributing to the report will get a copy, assuming that the final report is unclassified.

Thanks in advance. 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

# News from the KGB/Wily Hackers

Klaus Brunnstein <brunnstein%rz.informatik.uni-hamburg.dbp.de@RELAY.CS.NET> 07 Mar 89 18:52 GMT+0100

Now, 5 days after the 'sensational' disclosure of the German (NDR) Panorama TV team, the dust of speculations begins to rise and the facts become slowly visible; moreover, some questions which could not be answered (e.g. in Clifford Stoll's CACM paper) may now be answered. Though not all facts are known publicly, the following facts seem rather clear (most of the material has been published; I learned some facts when I analysed, for another Panorama story, some of the lists which had been sold to KGB, according to the journalists):

- In 1986, some hackers from W.Berlin and Hannover discussed, in 'hacker parties' with alcohol and drugs, how to solve some personal financial problems; at that time, first intrusions of scientific computers (probably CERN/Geneva as 'hacker training camp) and CCC's spectacular Btx-intrusion gave many hackers (assisted by newsmedia) the \*puerile impression\* that they could intrude \*into every computer system\*; I remember contemporary discussions on 1986/87 Chaos Computer Conferences about possibilities, when one leading CCC member warned that such hacks might also attract espionage (Steffen Wernery recently told that German counter-espionage had tried several times to hire him and other CCC members as advisors unsuccessfully).
- A 'kernel group' of 5 hackers who worked together, in some way, in the 'KGB case' are (according to Der SPIEGEL, who published the following names in its Monday, March 6 edition):
- ->Markus Hess, 27, from Hannover, Clifford Stoll's `Wily Hacker': after having ended (unfinished) his studies in Mathematics, he works as programmer, and tries to get an Informatics diploma at the University of Hagen (FRG); he is said to have good knowledge of VMS and UNIX (see Cliffs paper: it seems to give a good personal profile!).

- ->Karl Koch, 23, from Hannover, who works as programmer; due to his luxurious lifestyle and his drug addiction, his permanent financial problems have probably catalysed the desire to sell `hacker knowledge' to interested institutions.
- ->Hans Huebner, alias `Pengo', from Berlin, who after having received his Informatics diploma from Technical University of W.Berlin, founded a small computer house; the SPIEGEL writes that he needed money for investment in his small enterprise; though he doesnot belong to Chaos Computer Club (as he told me during last Chaos Computer Conference, December 1988), he holds close contacts to the national hacker scenes (Hamburg: Chaos Computer Club; Munich: Bavarian Hacker Post; Cologne: Computer Artists Cologne, and other smaller groups), and he was the person to speak about UUCP as a future communications medium (cf. my CCC'88 report in Risk Forum 89/01).
- ->Dirk Brezinski, from W.Berlin, programmer and sometimes `troubleshooter' for Siemens BS-2000 systems (the operating system of Siemens mainframe computers), who earned, when working for Siemens or a customer (BfA, a national insurance for employees) 20,000 DM (about 10,800 \$) a month; he is regarded (by an intelligence officer) as `some kind of a genious'.
- ->Peter Carl, from W.Berlin, a former croupier, who `always had enough cocaine'. (No information about his computer knowledge/experience available).

After successfully stimulating KGB's interest, the group (mainly Hess and Koch) committed their well-documented hacks (-->Clifford Stoll: `Stalking the Wily Hacker', CACM May 1988). SPIEGEL writes that the group \*sold 5 diskettes full of passwords\*, from May to December 1986, to KGB officers which they met in East Berlin; when Bremen University computer center, their favorite host for transatlantic hacks, asked (Dec.86) the police to uncover the reasons for their high telephone bills, they stopped the action.

This statement of Der SPIEGEL is probably wrong: as Cliff describes, the 'Wily Hacker' successfully worked until early 1988, when the path from his PC/telephone was disclosed by TYMNET/German Post authorities (the German public prosecutors didnot find enough evidence for a trial, when examining Hess' apartment; moreover, they had acquired the material in illegal actions, so the existing evidence couldnot be used and finally had to be scratched!).

In Hess' apartment, public prosecutors found (on March 3, 1989) password lists from other hacks. On Monday, March 6, 1989, the Panorama team (who had disclosed the NASA hack and basically the KGB connection) asked me to examine some of the password lists; the material which I saw (for 30 minutes) consisted of about 100 photocopied protocols of a hack during the night of July 27 to 28, 1987; it was the famous `NASA hack': From a VAX 750 (with VMS 4.3), which they entered via DATEX-P (the German packed-switched data-exchange network, an X.25 version), where they evidently previously had installed a Trojan horse

(UETFORT00.EXE), they tried, via SET HOST ..., to log-into other VAXes in remote institutes. They always used SYSTEM account and the `proper' password (unvisible).

[Remark: Unfortunately, DECs installation procedure works only if a SYSTEM account is available; evidently, most system managers do not change the preset default password MANAGER; since Version 4.7, MANAGER is excluded, but on previous VMS versions, this hole probably exists in many systems!]

Since the hackers, in more than 40% of the cases, succeeded to login, their first activitities were to SET PRIV=ALL; SET PRIO=9, and then to install (via trans-net copy) the Trojan horse. With the Trojan horse (not displayed under SHow Users), they copied the password lists to their PCs. When looking through the password list, I observed the well-known facts: more than 25% female or male first names, historical persons, countries, cities, or local dishes (in the Universities of Pisa, Pavia and Bologna, INSALATA was/is a favorite password of several people). Only in CASTOR and POLLUX, the password lists contained less than 5% passwords of such nature easy to guess!

Apart from many (about 39) unsuccessful logins, many different CERN /GENEVA, NASA systems (CASTOR, POLLUX, Goddard and Ames Space Flight Centers), several US, GB, French, Italian and some German institutes connected in SPANEt were 'visited'. The documented session was from July 27, 10 p.m. to July 28, 1 a.m. (I am not sure that I saw all the material available).

The media report that other hacks (probably not all committed by Hess and Koch theirselves) were sold to KGB. Among them, Electronic and Computer Industry seem to be of dominant interest for the USSR. If special CAD/CAM programs and Megabit designs (esp. from Thomson/France, from VAX systems) have been stolen, the advantage and value for the USSR cannot be (over)estimated.

In FRG, the current discussion is whether the hackers succeeded to get into 'kernel areas' or only 'peripheral areas'. This discussion is ridiculous since most 'peripheral systems' contain developments (methods, products) for future systems, while the 'kernel systems' mainly contain existing applications (of past architectures).

The well-known hackers (esp.CCC) have been seriously attacked by some media. My best guess is that CCC was itself \*a victim\* because the group succeeded to informally get much of the information which they needed for some of the hacks, and which they finally sold to KGB. Apart from 'Pengo', I dont see close relation between CCC and the KGB/Wily Hackers. Nevertheless, CCC and others, like Cheshire Catalyst in US, have prepared a climate where espionage inevitably sprang-off.

Klaus Brunnstein Hamburg/FRG.

# ✓ What's a hacker? (The fight to purify the word "hacker" is lost)

<ulysses!smb@research.att.com>Tue. 07 Mar 89 22:13:14 EST

I'm not sure we want to open this can of worms (again), but...

The grammatical world is divided into two camps on such questions, the prescriptivists and the descriptivists. The former know the "proper" usage for every word and phrase; the latter tell it like it is. To insist that "hacker" still retains its original meaning is to align yourself with the former camp. Face it, that battle is over, and the purists have lost; the word hacker, in many contexts, does now mean a criminal.

I've always been a descriptivist; trying to legislate how people talk is a singularly fruitless activity, the activities of certain governments notwithstanding.

--Steve BEllovin

# The fight to purify the word "hacker" is lost

Brad Templeton <br/>
<br/>
brad%looking.uucp@RELAY.CS.NET><br/>
Mon Mar 6 22:30:10 1989

It is with regret that I have to say that this fight has been lost. "Hacker" and "computer criminal" are now equated in the public mind, to the extent that this use of "hacker" now appears in newspaper headlines. The German Spy breakins confirm this in papers all over the world.

Once this has happened, we can't win the battle to get the old meaning back.

Who am I to announce the loss of this battle? A frontliner. My custom licence plate is "HACK." I got it back in the early days when it meant wizard. Sigh.

Brad Templeton, Looking Glass Software Ltd. -- Waterloo, Ontario 519/884-7473

#### False fire alarms

Peter Scott <PJS@grouch.JPL.NASA.GOV> Tue, 7 Mar 89 10:02:21 PST

A colleague just related a story to me about his apartment building. Recently the water main supplying the sprinklers fractured, some distance away from the building. The fire alarm is triggered by a drop in water pressure in the sprinkler system, on the thesis that a sprinkler has been set off. So the fire department arrived, but couldn't figure out why the alarms wouldn't shut off when no smoke alarms had been triggered, no call buttons had been pushed, no sprinklers were running, and there was nary a wisp of smoke.

Peter Scott (pjs@grouch.jpl.nasa.gov)

### ✓ Dangers of Spy programs

jpff@maths.bath.ac.uk <@NSS.Cs.Ucl.AC.UK> Tue, 7 Mar 89 18:10:54 GMT

The recent discussion of this reminds me of an incident which happened when I was a research student in Cambridge (way back..) when the computer we had was Titan. A staff member wrote a program (called L/WHO for other ex-Cambridge folk) which told who was logged on, and what they were doing. This was the first multiple access system in the UK, and so this kind of information was of great interest. A friend of mine, Robin Fairbairns, took the program an extended it to give more information, and we all enjoyed using it. One of his enhancements was to show which magnetic tapes a user had loaded.

Now the incident. The Titan Operating system scheduled tape jobs separately as tape decks were a scarce resource. In order to improve throughput the scheduler would accelerate starting jobs which used tapes which were already on a drive. Using the L/WHO program a student determined which tapes were in use, and used the information to get their programs run quickly. Of course the operators did not notice the effect, as the tape scheduling was totally automatic, and the cheating program did actually use the tape. That is until the day when the student program inadvertently wrote to block device zero, and as this was a tape (usually it would be scratch disk) the tape was overwritten. The owner of the tape was not amused at all (I will suppress the name as they are still very active). Robin was persuaded to remove the facility of giving tape names.

The operators objected of course. The operating system was not good at telling them which tape was where, and they had been relying on L/WHO for some time. The upshot was that the spy program had a "is this user the operator" function added (and also a "is this Robin F" bit). After that I believe it survived until the unfortunate switching off of such a great machine.

I will not attempt a moral, except to remark that the program did not use any privileged information. ==John ffitch

# ★ Re: reach out and spy on someone

vandenberg <vanden@studsys.mu.edu> 6 Mar 89 03:05:06 CST (Mon)

Although I'm not a UNIX guru (or even close for that matter) I do know that it is possible to 'monitor' someone else's terminal. With our setup, a 3b5 running SYS5, the defaults are such that anyone can 'see' what's on another terminal and even write to it. As one my guess this can lead to rather vicious games between bored students.

{..uunet..uwvax!uwmcsd1..}!marque!studsys!vanden {..uwvax..arpa..}!studsys.mu.edu!vanden vanden%studsys@marque.UUCP

#### Social effects of viruses

Don Alvarez <boomer@space.mit.edu>

Mon, 6 Mar 89 22:01:24 EST

"Guy\_Robinson.SBDERX<"@Xerox.COM writes about a Marvel Comics android(?) that gets wiped out by a computer virus and says:

>One problem this situation raised was that the Vision's human WIFE was a little >distraught! Could this be a whole new type of RISK to bear in mind?

I have a similar story from my own life, in which my roommate came home one night around 11:00pm to find me and my fiancee sitting, clearly very depressed, unhappily in the living room. He asked "what's the matter?" and my fiancee said "Don has a virus, and he just got reinfected, and there's nothing he can do about it." Needless to say my roommate felt this was not a good time to hang around and quickly disappeared. Only much later that night did he hear me on the phone to a friend in California (which was three hours behind us) and piece together that (a) I did not have any conventional social diseases (b) the infection was to my computer (c) the date was november 4th, 1988 (d) the virus was the "internet virus of 1988" and (e) the reason I couldn't do anything about it was that I couldn't get in as root over the modem. Talk about RISKS of computer viruses!

- Don

# ✓ Previous message to risks misunderstood (Power failure problems,

<ADEGROOT@HROEUR5.BITNET> Sat, 4 Mar 89 10:59 N

RISKS-8.28)

I received some flak from my previous employer after a message from me appeared in <u>risks 8.28</u>. Apparently they are even considering legal action ('though I'm not sure about this (yet)). I would like to set something straight...

- -I never mentioned the company's name in my message. Their view seems to be that this isn't necessary, as everybody knows I worked for them. I feel flattered, but I don't think it's true. I never had a function that exposed me to the public in any way.
- -They feel the message is degrading the company's image. Well, RISKS is meant as a forum to relate the risks of modern day technology to people professionally interested in those risks. It is not meant as a forum to make fun of companies ('listen what happened to them...'), nor of their employees. Despite this flak (which I consider to be a slight hiccup on their side), I still like the company very much, and I consider having worked with the people a great honour. I wouldn't think of insulting them in any way. They're great professionals, and I learned a lot from them. I also believe my message was received professionally by the Risks Forum, mainly because of the reply in RISKS-8.30 by Jonathan I. Kamens, relating a very similar case that happened to his University. If you feel I did degrade the company's image (and also happen to know the company's name), please send me a message. I would like to know how many people agree with my previous employer's views on this...

-John Sinteur (mail to adegroot@hroeur5.bitnet)

[RISKS Relevance sticklers may think that is not relevant. However, because of the obvious risks of sending contributions to public BBoards, it seems relevant enough to include. Please respond to John directly, although you may CC: RISKS-REQUEST (i.e., not for inclusion) if you wish. 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 8: Issue 37

# Saturday 11 March 1989

## **Contents**

- Computer blunders blamed for massive student loan losses **Rodney Hoffman**
- Prisoner access to confidential drivers' records **Rodney Hoffman**
- Ethics Question (Randall Neff) [Adobe rman?
- Risk of congenial machinery Robert Steven Glickstein
- Limitless ATM's
- **Geoff Kuenning** Re: Faking internet mail
  - Stephen Wolff
- Virus detector goes wrong **Dave Horsfall**
- Re: News from the KGB/Wily Hackers

<u>Hans Huebner = `pengo'</u>

- UK archive service [for European RISKS readers]
- Dave Ferbrache Info on RISKS (comp.risks)

### Computer blunders blamed for massive student loan losses

Rodney Hoffman < Hoffman. El Segundo @ Xerox.com > 10 Mar 89 14:48:43 PST (Friday)

Bank of America and possibly other major international banks stand to lose as much as \$650 million on bad student loans, due to computer problems at United Education and Software.

The 'Wall Street Journal' for Friday, March 10, provides the first hints of details I've seen on the nature of the "computer blunders" which earlier stories hinted at. The article, by Charles F. McCoy and Richard B. Schmitt, is headlined UNITED EDUCATION'S COMPUTER BLUNDERS FORM VORTEX OF BIG STUDENT LOAN FIASCO. Excerpts:

Computers at United Education and Software, Inc. ... ran wild for at least eight months. They rejected payments from overdue borrowers and addressed collection notices intended for New Yorkers to such places as "Radio City, N.Y.," among other gaffes. United Education and its colossal computer mistakes are at the heart of what is emerging as one of the most tangled loan fiascos in years...

The U.S. Dept. of Education has refused to honor guarantees on certain federally backed student loans serviced by United Education. That raises the possibility that BankAmerica or other banks that backed the loans with letters of credit will have to shoulder huge defaults. BankAmerica served as trustee on the loans... [Other banks, including Citicorp and several Japanese banks, dispute how much of the liability might be theirs, saying BankAmerica is responsible.]

United Education's beserk computer produced records that are so fouled up that nobody knows how much the losses eventually will be.

United Education and Software, oringinally a trade-school operator, began servicing student loans in 1983, and grew rapidly, developing a portfolio of more than \$1 billion in less than five years... The computer problems apparently stemmed from United Education's switch to a new system in October 1987. According to officials familiar with the problems, United Education's programmers introduced major software errors and failed to properly debug the new system.

Among the results, according to a Dept. of Education audit report:
United Education sent delinquency notices to students who were still
in school and thus weren't scheduled even to begin payments on the loans.
It placed students who were supposed to have been granted deferments
into default. It didn't inform many laggard borrowers that they were
delinquent, while informing some current borrowers that they were. The
computers also apparently logged telephone calls that were never made
and didn't log calls that were. United Education applied payments to
interest when they were supposed to be applied to interest and principal...

Aaron Cohen, president of United Education, called the depth of the problems identified by the audit a "shock." He said the company was aware of bugs in the new software that were causing accounting errors, but had no idea its loan servicing operation had run amok. He thought any problems were routine. "Software companies have problems all the time," he said...

#### Prisoner access to confidential drivers' records

Rodney Hoffman <Hoffman.ElSegundo@Xerox.com> 8 Mar 89 13:42:10 PST (Wednesday)

From a story by Leo Wolinsky in the 'Los Angeles Times' 5-March-89:

If the [California Governor] Deukmejian Administration has its

way, state prisoners soon will be put to work sorting through confidential motor vehicle records as part of the governor's plan to keep inmates working and save taxpayers money.

But the program, which is set to begin July 1, is prompting concern among some lawmakers and other officials who worry that the records -- which include names, addresses and some financial information about California motorists -- might end up in the hands of career criminals.

"The concept boggles the mind," said Assemblyman Richard Katz, chairman of the Transportation Committee. "They may be car thieves... They may have killed people or molested kids and now we're going to give them access to home addresses of people along with [information on] loans that they have on their vehicles and what cars they drive. It seems like an open invitation for trouble."

.... No one is sure what illicit uses, if any, inmates might make of the information. But the Legislature's nonpartisan analyst charged in a report that procedures employed by the state "may not be adequate" to ensure the security of the documents. "From our position, there is a fair amount that could be done even with this much information," said [one of the report authors]....

[In an earlier, now cancelled mail sorting job,] some corrections officers said they believe the inmates were searching for addresses of prison officials .....

PS. It is not clear from the newspaper article whether the records involved would be paper or on-line, so, strictly speaking, this may not involve any computer-based system RISK.

#### Ethics Question

Randall Neff <neff@paradigm.STANFORD.EDU> Fri, 10 Mar 89 17:28:55 PST

On Wednesday, March 8, Professor Michael A. Harrison, from the University of California, Berkeley, made a presentation: "VorTeX, a Multiple Representation System" to the Stanford EE 380/CS 540 Computer System Colloquium.

As part of the VorTeX project, the group decided that they needed a graphical display language, so they (re)implemented PostScript (trademark of Adobe Systems, Inc) on the Sun workstations. Then they realized that they also needed the fonts that are buried in the Apple LaserWriter. They talked to Adobe, but the money discussed was quite large (to Harrison) and he objected to Adobe's attitude (quote "shove in your face").

So, the group wrote several clever pieces of software (PostScript program to find the intersections of `scan' lines with the character boundaries, pump results back to Suns, program to curve fit the coordinates, etc.), and recreated the font information as Bezier cubic curves for use with their Sun

PostScript implementation.

According to the UC Berkeley lawyers, this is legal due to the current copyright law, that digital encoding of fonts is not protected by copyright. However, all Adobe sells is software and fonts; and the internal coding of fonts is a trade secret.

THE ETHICS QUESTION (I was really bothered by all of this):

Is this ethically correct?

Is it all right to acquire a company's product by clever coding?

Is it reasonable behavior for a Famous CS department funded by California taxpayers and NSF grants (it is certainly not research)?

Is there a reasonable way for an audience member to stand up and say:
"For Shame, this is ethically reprehensible behavior and you're setting
a bad example for students everywhere."

Randall Neff @ anna.stanford.edu

#### Limitless ATM's

<@sri-unix.UUCP, geoff@itcorp.com> Sat, 4 Mar 89 03:31:21 -0500

Like many people, I've occasionally wanted to get a moderately large amount of money out of an ATM, only to be foiled by a "daily limit" of some sort. I accepted this as a necessary evil for keeping thieves from completely cleaning me out.

Recently, however, I had an experience that taught me a possible way around these restrictions. A credit card and the associated PIN were stolen from my home, and the thief then used the card to withdraw \$3900 in cash from ATM's. Since the ATM's had a per-transaction limit of \$300, the withdrawal was done in 13 separate transactions. The interesting thing is that only two ATM's were used for all of these operations! Further, the card only had a \$3000 credit limit, and about \$600 was already in use. I don't know the reason for the lack of limits and restrictions, but I have begun to wonder just how much money I could get away with if I systematically spent a few days taking all my credit cards to ATM's and making withdrawals.

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

#### Risk of congenial machinery

Robert Steven Glickstein <bobg+@andrew.cmu.edu> Wed, 8 Mar 89 18:05:20 -0500 (EST)

An observation that I made earlier today:

I entered a store in the neighborhood with an old-fashioned mechanical cash register, complete with the little "I just made a sale" bell. I purchased an

item and after the transaction was complete, the clerk thanked me and wished me a good afternoon. I returned the pleasantry.

Later on I was in a much larger store, complete with barcode readers and electronic cash registers with dot-matrix LED displays. As the clerk rang up my purchase, the cash register told me "Thank You For Shopping At <Foo>" and my receipt said "Have a Good Day". Perhaps because the dreary task of being pleasant to customers was now automated, the clerk felt no need to greet me, address me, look at me, or in any way acknowledge me except to take my money and shove some change into my hand.

Computers do a lot of jobs a lot better than people, but there are some tasks that should be performed by no one but humans.

Bob Glickstein, Information Technology Center, CMU, Pittsburgh, PA

# ★ Re: Faking internet mail

Stephen Wolff <steve@note.nsf.gov> Thu, 9 Mar 89 14:59:33 EST

From "Kevin S. McCurley" <mccurley@IBM.com> in RISKS DIGEST 8.29:

- > I guess a lot of people know about faking Internet mail. Since the
- > National Science Foundation now accepts reviews of proposals via email, I
- > wonder whether anybody there knows about this?

Yes, we know. We also accept \*proposals\* electronically, so we have to face problems of privacy, too.

> It is rather farfetched to think that somebody would try to fake their > reviews,...

Nope, not at all.

These concerns are handled informally at present, but tighter methods are on the way.

### Virus detector goes wrong

Dave Horsfall <dave@stcns3.stc.oz.au> Wed, 8 Mar 89 12:45:17 est

Taken from "Computing Australia", Feb 27:

"Sneaky little non-virus

Sun Microsystems has moved to reassure Australian TOPS users that US reports on a virus are false. In a virus-paranoid environment, US pc users of TOPS/Mac Version 2.1 were running their disks through a virus detector before loading the software onto their computers.

It was a precaution that went wrong. The particular virus detector was Interferon and it falsely reported TOPS infected with a virus known as Sneak, said TOPS/Macintosh product manager Timothy Fredel.

Fredel said the resource structure of TOPS/Macintosh 2.1 happens to look like a Sneak virus to Interferon. To be on the safe side, Fredel suggested users run Virex or VirusRx."

So now one can't trust one's virus detector any more... On a different note, have there been any (confirmed) reports of a fake virus detector?

Ahhh, the perils of a standard Applications Binary Interface...

## ✓ Re: News from the KGB/Wily Hackers

Hans Huebner <pengo@netcs.SMTP> Fri, 10 Mar 89 18:09:25 MET DST

In <u>RISKS 8.36</u>, Klaus Brunnstein mentioned my name in the context of the hacker/espionage case recently discovered by the german authorities. Since Mr. Brunnstein is not competent to speak about the background of the case, I'd like to add some clarification to prevent misunderstandings, especially concerning my role. I think it is a very bad practice to just publish names of people without giving background information. Roy Omond did this once to a friend of mine, who has been a hacker as well, and his reputation in the net community has suffered from this publication quite a lot, even if he was doing a favour to the community by developing bug fixes and posting them to the net.

I have been an active member of the net community for about two years now, and I want to explicitely express that my network activities have in no way been connected to any contacts to secret services, be it western or eastern ones. On the other hand, it is a fact that when I was younger (I'm 20 years now), there has been a circle of persons which tried to make deals with an eastern secret service. I have been involved in this, but I hope that I did the right thing by giving the german authorities detailed information about my involvement in the case in summer '88. As long as the lawsuit on this case is not finished, I will/may not give any detailed about it to the public. As soon as I have the freedom to speak freely about all this, I'll be trying to give a detailed picture about the happenings to anyone who's interested.

For my person: I define myself as a hacker. I acquired most of my knowledge by playing around with computers and operating systems, and yes, many of these systems were private property of organisations that didn't even have the slightest idea that I was using their machines. I think, hackers - persons who creatively handle technology and not just see computing as their job - do a service for the computing community in general. It has been pointed out by other people that most of the 'interesting' modern computer concepts have been developed or outlined by people which define themselves as 'hackers'.

When I started hacking foreign systems, I was 16 years old. I was just interested in computers, not in the data which has been kept on their disks.

As I was going to school at that time, I didn't even have the money to buy an own computer. Since CP/M (which was the most sophisticated OS I could use on machines which I had legal access to) didn't turn me on anymore, I enjoyed the lax security of the systems I had access to by using X.25 networks. You might point out that I should have been patient and wait until I could go to the university and use their machines. Some of you might understand that waiting was just not the thing I was keen on in those days. Computing had become an addiction for me, and thus I kept hacking. I hope this clears the question 'why'. It was definitely NOT to get the russians any advantage over the USA, nor to become rich and get a flight to the Bahamas as soon as possible. The finish of the court trial will reveal this again, but until then I want to keep rumours out that the german hackers were just the long (??) arm of the KGB to incriminate western computer security or defense power.

It should also be pointed out that the Chaos Computer Club has in no way been connected to this recent case, and again, that the CCC as an organization has never been a 'hacker group'. The CCC merely handles the press for hackers, and tries to point out implications of computers and communications for society in general.

For punishment: I already lost my current job, since through the publications of my name in the SPIEGEL magazine and in RISKS, our business partners are getting anxious about me being involved in this case. Several projects I was about to realise in the near future have been cancelled, which forces me to start again at the beginning in some way.

-Hans Huebner pengo@tmpmbx, pengo@garp.mit.edu, huebner@db0tui6.bitnet

### UK archive service [for European RISKS readers]

Server <infoadm@cs.heriot-watt.ac.uk> 9 Mar 89 11:50:28 GMT

For the information of the European (especially UK) readers of the group, their is an archive of Comp.risks newgroup postings maintained on the Heriot-Watt information server.

The archive server is email based, and will accept requests in the form of an email message to <info-server@cs.hw.ac.uk>,with the text:

request: comp.risks

topic: v8.1

where topic can be either:

index for an index of all available risks digests (currently only v7.96 to date, I am hoping to extend this backwards to the time of the Internet worm).

v8.index for an index of all available digests in a specific volume

v8.contents for a list of the contents of all digests in a specified volume

(contents lists are extracted and appended as new digests are received and may thus be slightly disorganised)

v8.1 to send a specific issue (in this case digest 1 in volume 8)

any number of topics can follow the request. The server also archives virus-I digests, and holds BSD unix fixes, security software and virus disinfection software. For a general index of available materials, send a message of the form:

request: index topic: index

Dave Ferbrache Personal mail to:

Dept of computer science Internet <davidf@cs.hw.ac.uk>
Heriot-Watt University Janet <davidf@uk.ac.hw.cs>
79 Grassmarket UUCP ..!mcvax!hwcs!davidf

Edinburgh, UK. EH1 2HJ Tel (UK) 031-225-6465 ext 553

[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 8: Issue 38

# Wednesday 15 March 1989

## **Contents**

Water Bug - Computerization Messing Up Yacht Race

**Robert Horvitz** 

Sunspots & Communications

**Cliff Stoll** 

**PGN** 

pengo and the Wily hackers

Klaus Brunnstein

Toshiba DOS 3.3 Backup deletes files

Fiona M Williams

Star Trek computer virus

Kevin Rushforth

Re: NASA to replace top-level personnel with Expert Systems

**Henry Spencer** 

Pushbutton Banking

Lynn R Grant

Risks of telephone access to your bank account

Michael McClary

Limitless ATMs

John Murray

Re: Prisoner access to confidential drivers' records

Scot E Wilcoxon

Risks of Human Emulating Machinery

Jon Loux

New Sprint Card

Ken Harrenstien

Incoming-call identification

**David Albert** 

Info on RISKS (comp.risks)

# ✓ Water Bug - Computerization Messing Up Yacht Race

Robert Horvitz <rh@well.UUCP> Sat, 11 Mar 89 19:41:15 PST

An Irish friend, Derek Lynch, sent this article from the Irish Times' Sports page (10 Feb 89). Perhaps a British reader can provide the necessary follow-up:

"COMPUTER ERROR MAY PROVE COSTLY by Dermot Gilleece

"A major decision with critical implications for Ireland's first involvement in the Whitbread Round the World yacht race, will be taken in England next week. Race organisers, the Royal Naval Sailing Association, will be responding officially to a storm of criticism concerning the specifications of competing yachts...

"The problem concerns the technique of measuring yachts which, in the context of the Whitbread Race, are in the maxi, 70 foot class. This is the responsibility of the British-based Offshore Racing Council, which introduced a new measuring process two years ago.

"Up to that stage, yachts were hand-measured, taking various complex factors, even the size of the engine, into the equation. It was then decided that computers could handle the process more efficiently.

"In the event, a fault was discovered in the computer software with the result that specifications were more liberal than intended. So, the Offshore Racing Council corrected the error last November.

"By then, however, two New Zealand yachts had been built according to the faulty computer measurement... The fact was that, while the New Zealand yachts measured 70 feet under the faulty process, their actual measurement was 71 feet.

"The implications of this discovery were far-reaching. Rear-Admiral Charles Williams, chairman of the race committee, was bound by the new regulations which, in effect, made the New Zealand craft illegal. On the other hand, if the New Zealand yachts were accepted into the Whitbread Race, they would have a decided advantage over British and Irish craft - possibly by as much as 10 hours in the 36,000 miles event, which will get under way in September...

"Butch Dalrymple-Smith is a partner in the company of Ron Holland, the Cork-based designer of NCB Ireland. He said last night: `My view is that the New Zealand boat which we know to be outside the limit, was built with the computer loophole in mind.

"`We knew about the problem as far back as last July when the Americans decided that yachts built to the faulty computer process were unacceptable. Admittedly NCB Ireland was built at that stage but we could still have carried out the necessary modifications had we needed to..."

"It has been suggested that Rear-Admiral Williams has bowed to pressure from the New Zealanders, who are heavily sponsored. This was roundly rejected last night by Captain Brian Evans, the race secretary...

"He added: `The matter will be cleared up next week when we will be announcing our decision.'...

"If NCB Ireland were to be modified to make it competitive with the New Zealanders, the expense would be formidable. For instance, a new keel would cost L/40,000, a mainsail L/10,000 and a new rig as much as L/150,000.

"At this stage, it would appear that the RNSA will have no option other than to back down in the face of overwhelming protests... Meanwhile, leading yachtsmen will be awaiting next week's decision with some apprehension. This is clearly a case in which a considerable quantity of oil will be necessary to calm troubled waters."

#### Sunspots & Communications

Cliff Stoll <cliff%cfa204@harvard.harvard.edu> Mon. 13 Mar 89 13:55:36 est

There's a major sunspot group on the sun ... it's visible to the naked eye (with suitable protection, of course). Largest sunspot in a long time. At least two flares have been associated with this group.

Ten or twenty years ago, we'd probably have heard warnings that communications circuits might be disrupted, due to ionospheric interactions with the solar wind.

Today, however, it's a rare communication link that depends on ionospheric reflections (although military over-the-horizon radars do...).

So this sunspot won't affect our communications, huh? You say we've nothing to worry about?

Maybe. Here's a few things to worry about:

- 1) Geomagnetic storms can screw up magnetic compasses.
- 2) Satellites in geosynchronous orbit have a rough time of it. Twice a year, (at each equinox), they're shadowed by the earth, and their solar panels don't generate electricity at night. In addition, the high energy particles can get wicked at this altitude, especially when there's a major solar flare. Well, it's near the equinox (so the comsats are battery powered at night), and there's bad solar flares. Result: these satellites are being stressed.
- 3) Earth satellite lifetimes depend on the shape and size of the earth's atmosphere. Satellites in low orbits may have their lifespans shortened drastically when the atmosphere bulges out. What causes such bulges? Increased solar activity.

If this sunspot -- largest in memory -- is an indicator of a very active sun in the next few years, low-flying satellites may be in trouble.

Best of cheers, Cliff Stoll cliff@cfa200.harvard.edu 617/495-7147 Smithsonian Astrophysical Observatory Harvard - Smithsonian Center for Astrophysics

### Sunspots & Communications (O Solar Milhaud!)

Peter Neumann <neumann@csl.sri.com> Wed, 15 Mar 1989 9:28:47 PST

Solar flares resulting from the unprecendented sunspot activity have reportedly been wreaking havoc with communications around here since about 10 March. (And the peak of the 11-year sunspot cycle is still about a year away!) Radio and satellite communications have been seriously affected. In the Mount Diablo area of California, there have been many reports of garage door openers failing to operate. (Younger RISKS readers will not remember a different effect caused by signals from the first Sputnik, which merrily opened and closed garage doors each time it traversed the U.S. -- at the time there was little redundancy in the g.d. control signals. This time the controls are apparently being jammed.)

[The "Subject:" line subtitle is due to the fact that I had awful radio reception on hearing a piece by Darius Milhaud.]

[By the way, today is the day to "Beware The Ides of March", which means that The Calends of April is only 17 days away. As we have learned, Beware the Calends of April also.]

### pengo and the Wily hackers (RISKS-8.37)

Klaus Brunnstein <brunnstein%rz.informatik.uni-hamburg.dbp.de@RELAY.CS.NET> 14 Mar 89 11:04 GMT+0100

In RISK FORUM 8.37, 'Pengo' Hans Huebner stated that he had no share in the KBG case as I mentioned in my RISK report. Since I myself had no share in the KGB hack (and in this sense, I am not as good a source as Pengo!), I tried to transmit only information where I had at least \*two independent sources\* of \*some credibility\*. In Pengo's case (where I was rather careful because I could not believe what I read), my two sources were:

- the SPIEGEL report (I personally agree that names should be avoided as long as current investigations are underway; yet in this cases, the names have been widely published in FRG and abroad);
- a telephone conversation with a leading CCC person (before I present his name, I will inform him); after he had informed me about a public debate at Hannover fair (where the German daily business newspaper, Wirtschaftswoche had organised a discussion with data protection people and CCC), I asked him whether he knew of Pengo's contribution; he told me that he directly asked Pengo: '`Did you, without pressure and at your own will, work for the Russians?', and Pengo answered: 'Yes'. He told me that he immediately cut-off any contact to Pengo. Evidently, there was a

controversial discussion in Chaos Computer Club whether on should react in such a strict manner. I understand the strong reaction because the KGB hackers severely damaged CCCs attempt to seriously contribute to the public discussion of some of the social consequences of computers. They now face, more seriously than before, the problem of being regarded as members of a criminal gang.

In the bulk of information, I found much desinformation (not only regarding computer stuff, like the notion of a sold `C-Compiler, which is a program to accomodate old programs to modern computers'). I didnot mention such desinforming non-facts (like the rumor that also personal information was sold) because I had only one source, which moreover was of very limited credability.

Klaus Brunnstein

#### Toshiba DOS 3.3 Backup deletes files

Fiona M Williams <fiona@euroies.ucd.ie> Tue, 14 Mar 89 14:34:50 GMT

A colleague of mine had just started to backup the hard disk of his Toshiba 3200 using the Toshiba DOS 3.3 backup command. While backup was still looking at the root directory we had a power failure in the office. A couple of gnashes later he re-booted the T3200 only to get the message "Bad or missing command interpreter." (This generally means that command.com has been knackered.) Also, when we looked at the backup diskette, there was nothing on it!

Having (eventually) found a Toshiba DOS 3.3 diskette we managed to have a look at the hard disk only to find that all files in the root directory \*had been deleted\*. (Sub-directories were ok though.) Norton's quick un-erase came to the rescue so we managed to recover everything after about an hour.

I'd hate to think what might have happened if we'd had the power failure when backup was on its 20th diskette, rather than its first, but in any case, the moral seems to be that you should sometimes make a backup before making a backup!

Stephen Farrell, MANTIS LTD. (stephen\_farrell\_mantis@eurokom.ucd.ie)

#### Star Trek computer virus

Kevin Rushforth <kcr@Sun.COM> Tue, 14 Mar 89 22:30:12 PST

I realize that the fictional world of Star Trek is not normally an appropriate risks topic, but I feel this is an exception. The next original episode of "Star Trek: The Next Generation" (scheduled to air the week of 3/20-3/26) is titled "Contagion" and is about (you guessed it) a computer virus:

The Enterprise's computer system falls prey to a mysterious electronic "virus" which programs the ship to self destruct.

This episode may prove interesting to readers of comp.risks. It raises an interesting question as to what would happen if the on-board computer of an F-16 or Space Shuttle were to contract a virus.

Kevin C. Rushforth, Sun Microsystems

#### Re: NASA to replace top-level personnel with Expert Systems

<henry@utzoo.UUCP>
Sun, 12 Mar 89 01:33:01 -0500

A cynic might say that replacing many of NASA's top-level people with, say, a PC each would be an \*improvement\*, bugs and all... Let us not forget that some human beings are far from fully debugged. Today's NASA is notorious for bad management (e.g. Challenger) and too much management (NASA's supervisor:worker ratio today is twice what it was during Apollo). If nothing else, a program spouting nonsense is easier to ignore than a manager spouting nonsense -- programs have less political clout.

Henry Spencer at U of Toronto Zoology uunet!attcan!utzoo!henry henry@zoo.toronto.edu

# Pushbutton Banking

Lynn R Grant <Grant@DOCKMASTER.ARPA> Wed, 15 Mar 89 14:00 EST

My bank, the Suburban Bank of Palatine (Illinois) has just announced that starting April 1st (April Fool's Day!) they will be implementing "Pushbutton Banking," which will allow you to query balances, find out what checks have cleared, and transfer balances between accounts, all from the comfort of your easy chair, using your Touch-Tone phone.

All you need to access this is your account number and your security code, which is the last four digits of your SSN. I called the bank and asked them if the security code was changable by the user. They said no, but how many people know your account number and SSN. I pointed out to them that since my Illinois driver's license has my SSN on it, every time I pay by check at a store, I am showing the cashier my account number and SSN. The bank said that that hadn't occurred to them. They offerred to set up my account so that nobody, including me, could use the pushbutton banker on it, and of course, I accepted.

It is certainly worrysome that the people charged with keeping my money safe don't think about these things. True, the pushbutton banker could probably not be used to steal money, but it could certainly invade your privacy, and could be used to perform denial-of-service attacks (someone dials in and transfers all your checking account money to your savings account, causing all your checks to bounce. The merchants you paid by check all charge you their 10 or 20 buck returned check fee. When you try to explain your way out of the charges, the bank says "Well, it must

have been you; who else would know your account number and security code?").

--Lynn Grant

## Risks of telephone access to your bank account

Michael McClary <michael@xanadu.com>
15 Mar 89 13:13:05 GMT

Upon moving to California, I opened an account at a local bank (Wells Fargo). They took down a bunch of personal information to use to identify myself when using their 24-hour telephone account-munging service. The information was a standard set, such as mother's maiden name. All public record, as I recall, but in any case nothing a cheap private detective couldn't dig up, given a little time. So anyone who'd, say, gotten hold of my checkbook, could find out how much it was good for.

But the surprise came when I was back in Michigan finishing the move, and needed to transfer funds to cover a check. Instead of a random set of the items, they asked for EVERY SINGLE ONE of them. Anyone listening in on the phone would have all they'd need to use the service.

Now combine that with cellular phones that:

- are not scrambled,
- don't switch channels enough to break up a conversation,
- can be recieved on the high end of an old TV set's UHF dial
- are generally owned by busy people with money and you've got the makings of some nasty surprises.

#### ✓ Limitless ATMs (Re: RISKS DIGEST 8.37)

John Murray <johnm@uts.amdahl.com> 15 Mar 89 20:43:27 GMT

> From: @sri-unix.UUCP, geoff@itcorp.com

>

- > . . . . A credit card and the associated PIN were stolen from my
- > home, and the thief then used the card to withdraw \$3900 in cash from ATM's.
- > Since the ATM's had a per-transaction limit of \$300, the withdrawal was done in
- > 13 separate transactions. The interesting thing is that only two ATM's were
- > used for all of these operations! Further, the card only had a \$3000 credit
- > limit, and about \$600 was already in use.

Several ATM systems have (used to have?) loopholes in them, which allowed this type of thing to occur. For example:

\* In regions where on-line links are unreliable, a machine might use floppy disks for its data. The transaction file and "hot-card" data are only updated once a day, and the bank moves this info using its regular courier system. All sorts of risks can occur over public holiday weekends.

- \* The card in question is a credit card. It seems unlikely that data for ALL cards EVER issued ANYWHERE is instantly available EVERYWHERE, especially across international boundaries. Perhaps some systems just accept this potential for loss.
- \* Some off-line systems could rewrite data onto the card, so that taking the card to a different machine wouldn't work. However, using joint cards could not be trapped.
- John Murray, Amdahl Corp. (My own opinions, etc.)

#### Re: Prisoner access to confidential drivers' records

Scot E Wilcoxon <sewilco@datapg.mn.org>
14 Mar 89 05:42:21 GMT

Much of the information which was mentioned is already easily available. For \$3, the California DMV will give you auto registration information. "Names, addresses", and "what cars they drive" certainly, and maybe also "loans" (I forgot to ask the DMV about loans, but I know Minnesota lists loan info). Auto and driver registration information is public in most states.

Apparently the California government has considered the license holders' desire for privacy (or perhaps of the ignorance of the public status of the information). Along with the \$3, you must give a signed statement of the reason why you want the information. The license holder then is notified by mail that the information was delivered, and of the reason you gave.

Scot E. Wilcoxon

### Risks of Human Emulating Machinery

Jon Loux <JLOUX@UCONNVM.BITNET> Mon. 13 Mar 1989 09:59:51 EST

In reply to "Risks of Congenial Machinery" from Robert Steven Glickstein. Hear, hear. In the effort to make our machines more like humans, we have failed. The best we can do is make a parroting parody of some intellectual function. Useful? Yes. Important? Yes. Vital to the functioning of many (most) institutions in our society? Yes. But human? No. We cannot make our machines more like humans, so we have done the next best thing. We have made our humans more like machines. The silicon revolution is nothing more than the industrial revolution without the smoke. Mechanized. Mass produced. And impersonal.

A case in point. A senior project manager in the DP shop of a large defense contractor told me a story about his home bank back in the town in New York where he grew up. It used to be that the tellers and managers of the bank knew everybody in the town. If a check came in without sufficient funds in

your account to cover it (Banks don't like this, for some reason) they would call you at work and make some arrangements for you to cover it (run down and make a deposit, hold the check, whatever). It was a community matter. Now, with ATMs and electronic funds transfers, etc., walking into the bank is the financial equivalent of entering a meat locker.

"But Bob," I said. "The bank must be serving a larger number of people. It's just impossible to be personal in a corporate setting. This isn't Bailey's Savings and Loan, you know."

"No," he said. "But the town's population hasn't gone up in fifty years."

You decide.

Jon Loux. University of Connecticut.

# New Sprint Card

Ken Harrenstien <KLH@SRI-NIC.ARPA> Thu, 9 Mar 89 13:23:18 PST

Regarding the message from Will Martin:

... Fred Lawrence, Sprint's executive vice president for network development, said the Voicecard would work a little like the company's Foncard: Callers dial the phone number printed on the card, adding a second number such as a birthdate, and then give a two-second verbal password. Sprint equipment compares the voice print with one that is on record. The call goes through only if the voice prints match, Lawrence said. ...

My hair rose when I saw this. I may be over-reacting in the absence of additional information, but I sincerely hope this idea does not spread. If it did, I won't be able to make a long-distance call, because I'm deaf.

Let me explain for the benefit of people who don't get it. How could deaf people make calls in the first place anyway? There are normally two ways:

First, they can use TDDs (Telecommunication Device for the Deaf). This is typically a small terminal-like unit that uses half-duplex FSK (1400/1800 Hz) to transmit Baudot codes at 45.45 baud. More foresighted designs also provide the capability of using ASCII with a standard 300 baud (Bell 103) full-duplex modem. People can thus type to each other.

Second, they can use an interpreter -- the usual resort when one of the parties is hearing and doesn't have a TDD. But it's very rare that one can use the same interpreter (i.e. the same voice) every time.

Perhaps the Sprint people have thought about this, and have an alternate security method for those cases. But I rather suspect not. I don't have any problem with proposals for whiz-bang new techno-fixes that are focused on just one modality, but all too often these ideas unwittingly exclude other modes, which is exactly the wrong thing to do where a public service is concerned.

Think about color-coded displays. Touch displays. Mice. Voice-synthesized responses. And so on. None of these is suitable for everyone, but as long as a system is not limited to just one way of doing things, no one will be excluded. I sincerely hope that in the rush to automate everything, designers take advantage of the flexibility that computers give them to provide for as many alternatives as possible. The person who benefits will someday be you. --Ken

# **★ Incoming-call identification**

David Albert <albert@harvard.harvard.edu> Thu, 2 Mar 89 19:04:57 EST

Today's (3/2/89) Boston Globe has an article on telephone features, including incoming-call identification. I quote a relevant section:

[Spokesperson for Bell Atlantic Karen] Johnson ... brushed aside questions about the privacy of incoming callers. "We feel that in most cases, the caller gives up anonymity and the customer gains privacy and security. In all the time we've offered it, we've had very few complaints."

New England Telephone's [product manager for the new calling services Gerald J.] Malette agreed. "We feel the person being called has the right to know who's calling," he said.

Well, we keep bringing up the issue on the net; perhaps it's time we started complaining directly to the people keeping track of the number of complaints, such as the two named above. In particular, I suggest we bring to their attention the issue of the confidentiality of calls to services such as the Samaritans, to the police (on their business number), to the government (say, asking questions about tax laws), and to businesses in general. Do we really want to give up our privacy when a business might turn around and compile a mailing list (or worse, a calling list) based on telephone calls received?

When we want to ask an anonymous question of a government agency? When we are baring our souls to a suicide line? Let's all get out there and complain before it's too late (if we're not too late already).



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 8: Issue 39

# Thursday 16 March 1989

#### Contents

Solar flares vs. garage door openers

Steve Bellovin

Peter Scott

Sunspots and Power Lines

John Coughlin

Man-machine interfaces and perception-impaired people

David A. Honig

Re: reverse engineering of type fonts

Herman J. Woltring

Re: Ethics Question

**Marc Mengel** 

Re: Toshiba DOS 3.3 Backup deletes files

Jav Elinsky

Re: IBM's claims to omnipotence

**Dr Robert Frederking** 

Re: Pushbutton Banking

Tom Coradeschi

Info on RISKS (comp.risks)

#### Solar flares vs. garage door openers

<ulysses!smb@research.att.com> Thu, 16 Mar 89 10:40:37 EST

You write that the solar flares have been affecting garage door openers. Maybe not. According to a report on CBS News this morning, the FCC is aware of the problem, refuses to say what it is, but says it will clear up in about 6 weeks. When asked if it's a secret government project, they refuse to say.

The transmissions are from the top of Mount Diablo, but the FCC [office in Livermore] refuses to identify the agency sending. They'll be transmitting through May 2. Quoth an FCC representative: "We're not obligated to do anything" because the openers operate on frequencies also used by the government, and the openers are "unprotected devices". His solution: switch to another frequency.

I wonder what other equipment, besides garage door openers, is failing? And if they -- whoever ``they'' are -- even thought about the question first?

Steve Bellovin

[This report was also noted by Jan Wolitzky and Tim Garlick. Also, Michael Sclafani -- who had not heard it -- wondered how a solar flare problem could arise only in the Mt. Diablo area. PGN]

### Re: Sunspots & Communications

Peter Scott <PJS@grouch.JPL.NASA.GOV> Thu, 16 Mar 89 09:30:38 PST

[...] I thought that g.d. openers operated in the microwave range; isn't this power level of transmission unhealthy?

Peter Scott (pjs@grouch.jpl.nasa.gov)

[Especially if you jack up the power. You need jacks or better to open. PGN]

# Sunspots and Power Lines

John Coughlin <John\_Coughlin@RMC.BITNET>
16 Mar 89 12:19:00 EST

Earlier this week a massive blackout hit the province of Quebec, plunging about 6 million people into darkness. A substation on one of the main lines feeding electricity from the James Bay hydroelectric dams to the south of the province had shut down. The suspected reason: the recent intense solar activity. It took almost half a day to rectify (pun intended) the problem, because it was first necessary to identify which of several substations located in a remote area was at fault.

John Coughlin, BULL Kingston (613) 541-6439 <JC@RMC.BITNET>

#### man-machine interfaces and perception-impaired people

"David A. Honig" <honig@BONNIE.ICS.UCI.EDU> Thu, 16 Mar 89 12:36:00 -0800

In RISKS [ Wednesday 15 March 1989 Volume 8 : Issue 38 ] Ken Harrenstien <KLH@SRI-NIC.ARPA> writes,

Think about color-coded displays. Touch displays. Mice. Voice-synthesized responses. And so on. None of these is suitable for everyone, but as long as a system is not limited to just one way of doing things, no one will be

excluded. I sincerely hope that in the rush to automate everything, designers take advantage of the flexibility that computers give them to provide for as many alternatives as possible. The person who benefits will someday be you. --Ken

The developers of advanced man-machine interfaces who wish to use stereooptical displays (so users can manipulate virtual 3-D objects) will have to contend with the fact that approximately 10% of the population has some form of stereodeficiency (usually caused by eye problems as an infant). Groups at NASA, MIT Media Lab, etc. have working prototypes, and it is common for CAD/CAM users to employ 3-D computer graphics.

David Honig, Dept of Info & Comp Sci, Univ. of Calif., Irvine, Ca. 92717

## ★ Re: reverse engineering of type fonts (Herman J. Woltring)

<WWTMHJW@HEITUE5.BITNET> Thu, 16 Mar 89 12:03 N

Mr Randell Neff's query in Risks Digest 8(37) of March 11, 1989 on the ethics and legality of investigating a commercial object and of recovering some of the basic information incorporated in such an object (type fonts information in his paradigm) seems to have a direct bearing on my own (too lengthy) contribution in Risks Digest 8(34) of March 2, 1989. The French proverb "C'est le ton qui fait la musique" (i.e., the way that you put your arguments will have a strong bearing on how your views are perceived and interpreted) may be relevant, as Mr Neff's statement seems to convey that the VorTex people were boasting about their success in avoiding payment of (too) much money. If this was indeed the case, no wonder that some people including Mr Neff became rather upset.

Apart from such psychological factors, the legal and ethical aspects might be discussed as follows. I should state that I am neither a lawyer nor an ethicist, but just a computer architect interested in balancing Intellectual Property with Freedom of Information, considering the complementary nature of these aspects under Section 27 of the 1948 Universal Declaration of Human Rights and under Section 15 of the 1966 International Covenant on Economic, Social, and Cultural Rights.

Under most legislation in competitive economies, investigating some commercial object by disassembling it for one's own purposes is perfectly ethical and legal. It is only once a direct-for-profit goal becomes the target, that patent law etc. impose certain constraints. Freedom of Information, especially in the USA with its Freedom of Information Act, is an important asset that should not be forgotten lightly.

If disassembling a (purchased or borrowed) object for research on its functioning and properties is acceptable in a competitive context, why should it become inacceptable if done in a not-for-commercial-gain context? Mr Neff referred to trade secrets of the font information incorporated in Adobe's product, and this ties directly into the present, commercial drive to use copyright law for imposing trade secrecy on the fundamental know-how contained in a (software) object. However, trade secrets must be KEPT secret, e.g., by

binding human persons in contract and by storing documents in strong vaults. It does not make sense to rely on legal connotations that "reverse engineering" of an object (whether hardware or software) are inappropriate and an intellectual burglar's instruments for "theft of know-how": research is allowed on the topography of hardware chips and under patent law (but licences may be imposed once the results of such research are to be exploited commercially); similar research should remain possible under copyright law. This obtains even more because of the automatic, virtually costless protection granted by copyright; patent law requires rather expensive, administrative procedures.

As I am most familiar with the software aspects, I'd like to clarify things in the software area, although I do not know whether the VorTex/Adobe controversy is a hardware or a software issue. Higher computer languages exist in order to accomodate the cognitive capabilities of the human computer architect and programmer, and machine languages exist in view of the limitations of current hardware technology. The gap between these two is bridged by compilers and decompilers, and compilers have never been designed in order to impose secrecy of the know-how underlying a software package. Thus, decompilers are not automatically improper tools.

Nevertheless, a number of creative legal experts consider it useful for their own purposes to declare decompiling and similar forms of analysis and research first an unethical, then a pirating, and finally an illegal activity. However, the mere fact that there is a new market for something (software used to be freeware!) does not automatically imply that existing tools and technologies should be reinterpreted as legal instruments. Such political interpretations should be judged in terms of the necessary balance between protection and freedom to copy, lest inappropriate monopolies (and similar advantages) are generated or no protection is provided at all.

For example, the "Green Paper on Copyright and the Challenge of Technology" published by the Commission of the European Community last summer makes specific reference to the information industry's need that reverse engineering should be allowed lest competition would be stultified: in each competitive situation, we may copy relevant aspects from our competitors (not slavishly, but creatively, by building on those predecessors' work), and this should certainly remain pos- sible. Balance and counterbalance must, of course, be provided, and the copyright doctrine that only form or expression, but not basic ideas or contents are to be protected, is one of the tools for that purpose. In my mind, this means that a legal "fair use / fair dealing" exemption for research, review, and criticism of a protected object should be maintained, but that unfair uses should be outlawed. (The national motto "Je Maintiendrai" of the Kingdom of The Netherlands may be of some relevance, here.)

Case law under the Anglo-American Copyright system has been perfectly capable to interpret the extent of (un)fair behaviour, whether commercial or consumptive. The non-competitive VorTex case seems quite within the range of what is called "Fair Use" under Section 107 of the US Copyright Act. In fact, Mr Neff did not clarify his claim that the VorTex activity with respect to Adobe was "certainly not research", as VorTex seemed concerned with saving money for research purposes; rather, the VorTex group might deserve to be congratulated with saving the Californian and other taxpayers' money? After

all, the VorTex group did not slavishly copy a protected object for its own, routine use, but analyzed it and then built its own version instead. The similarity to industrial 'clean room' procedures where (computer) architects analyze an object and provide their findings to an independent, 'clean' team of programmers or hardware engineers may be obvious.

As regards copyright protection of digital encoding of fonts, I doubt that this does not exist in the USA. Certainly, the 1988 Copyright, Designs and Patents Act in the U.K. provides for specific Copyright protection of typefaces and print lay-outs. Much more serious is the possibility that the VorTex group (if Fair Use under Section 107 USC Copyright Act should not apply) might invoke the 11th Amendment to the US Constitution which grants individual States (including State instrumentalities like the University of California at Berkeley) immunity against copyright damage claims under the federal Copyright Act: see the paper "An Open Letter on Piracy" in Software Magazine 8(3) of March 1988, republished in ACM's Computers and Society 18(3) of July 1988, also referred to in my Risks posting of March 2, 1989 quoted above.

Finally, I hope that Mr Neff has communicated his feelings to the UCB professor of whom he was so critical, and that a reaction may appear from him on this forum; I hope that such a communication took place prior to Mr Neff's going public on this issue.

Herman J. Woltring

# ★ Re: Ethics Question (Randall Neff, RISKS-8.37)

<att!cuuxb!mmengel@ucbvax.Berkeley.EDU> Mon, 13 Mar 89 23:59:59 -0800

>Is this ethically correct?

Copyrights and intellectual property are a very sticky issue... especially in a case like this.

Consider: Adobe's \*internal coding\* of the fonts is considered a trade secret, and that trade secret has \*not\* been abridged by digitising the display of the font. The display of the font was performed by the group's equipment, and with electricity for which they paid... If I buy a machine that makes pretzels, may I not sell the pretzels?

Lets say I write a book, printed with Adobe's fonts -- can I sell copies of the book? Or must I purhcase the font from Adobe for large sums of money?

>Is it all right to acquire a company's product by clever coding?

Clearly not, if you mean breaking some form of computer security to obtain copies of the software, etc. On the other hand, to build your own product that acts like another company's is quite the proper thing to do. Just ask Suave shampoo. ("Ours does what theirs does...") Or your local pharmacist who makes generic versions

of common brand name pharmaceuticals.

It is the latter course that the CS department has followed, in my opinion.

>Is it reasonable behavior for a Famous CS department funded by California

> taxpayers and NSF grants (it is certainly not research)?

I find your assertion questionable -- after all, universities design operating systems, and aren't there operating systems being sold by companies? Don't features of those operating systems get put into these research systems by "clever coding?"

If you want to, you can make any research implementation of anything which has been previously built in industry sound like some sort of copyright violation; just say that the products do similar things, and the students managed to "reproduce" the package with "clever coding"... Never mind if the researchers happen to stumble upon a signifiganly improved method of getting the job done, or learn something usefull about software engineering...

>Is there a reasonable way for an audience member to stand up and say:

- > "For Shame, this is ethically reprehensible behavior and you're setting
- > a bad example for students everywhere."

Not unless you can first demonstrate that the behaviour is morally reprehensible. When you can do that, you need merely ask a few pointed questions of the presenters, and the conclusion will be obvious to the other listeners.

However, from the way you describe it, they wrote their own implementation of Postscript, a programming language in its own right, with their own code for displaying fonts, etc. and then wrote a program that could digitize characters which were to be displayed on their printer, and could digitize \*any\* font displayed on that printer, even one they might have done by hand; they then used this tool to digitize a font they had purchased the right to reproduce in its displayed form (It would be ludicrous to suggest they need an incredibly expensive liscence just to make photocopies of documents printed on their printer, for example).

They rewrote Postscript, and digitized some fonts for its use. They could just as easily have run the New York Times through a scanner and picked the letters from it, or typed the alphabet on their typewriter and scanned it in with a digitizer. The typewriter company sells those printwheels for the typewriter; but have our proponents done anything ethically abhorrent? I don't think so.

Marc Mengel

### ★ Re: Toshiba DOS 3.3 Backup deletes files

"Jay Elinsky" <ELINSKY@YKTVMX.BITNET> Thu, 16 Mar 89 08:56:31 EST

Stephen Farrell writes

>the moral seems to be that you should sometimes make a backup before making a >backup!

It's "standard practice" to keep at least two sets of backups. Call one set of diskettes A, and the other B. This week write your backups on set A. Next week write them on set B, and then back to set A, etc. If your machine dies in the middle of writing on set B, you have some hope of restoring from set A (the backup you took a week ago).

The UNIX manual page dump(8) tells about a hierarchial dumping scheme in which you keep some backups forever.

Jay Elinsky, IBM T.J. Watson Research Center, Yorktown Heights, NY

### ★ Re: IBM's claims to omnipotence (RISKS-8.32)

Dr Robert Frederking <ref@ztivax.siemens.com> Mon, 13 Mar 89 14:49:16 -0100

- (1) Why these things always go IBM's way in the press:

  IBM probably has more PR people than most companies have programmers.
- (2) My biggest complaint about an article like this is that apparently no one, including the reporter and the poster to this list, remembers that the first(?) launch had to be rescheduled because of a complete computer system failure in the flight-control computers! This, in a "bug-free" system. It turned out that there was a 1-in-64 chance (really!) of the system not synchronizing on start-up. Once it hit the bad combination, it had to be reset before it would correctly synchronize. This wasn't discovered in testing because they were too busy testing software in the individual machines to keep cold-starting the whole system. The whole thing had been started from scratch less than 10 times.

Robert Frederking, Siemens AG/ZFE F2 INF 23, Otto-Hahn-Ring 6, D-8000 Munich 83 West Germany Phone: (-89) 636 47129

#### Re: Pushbutton Banking

Tom Coradeschi <tcora@ARDEC.ARPA> Thu, 16 Mar 89 18:27:21 EST

In a similar vein, the credit union here, at ARDEC has a system much like that you've described. It is somewhat safer, however. The ID number you use is your choice, not something nominally available to the public, like your SSN. It is

not possible to transfer funds OUT of checking, to savings or elsewhere. It is possible to transfer funds into checking, but that's what you want to do, anyway. The only possible means of screwing someone over, I can think of, would be to locate both his account number and ID number, and make a withdrawal. However, the method of withdrawal the credit union uses is to mail a check to the address of record for the account. And there is no way to change your address using the phone. That requires an in-person visit, with account identification. If you've got that, why bother using the phone, when you can walk up to a teller window and clean out the account? I'm sure that there are some bugs in this system as implemented, and someone who was really trying could find them, but they certainly aren't as readily apparent as those described earlier.

tom c

Electromagnetic Armament Technology Branch, US Army Armament Research, Development and Engineering Center, Picatinny Arsenal, NJ 07806-5000



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 8: Issue 40

# Friday 17 March 1989

# **Contents**

Re: Sunspots & Communications Jordan Brown

Gasbarro

Ethics of Copying Fonts

Jerry Schwarz

Policy Statement Request

**Dave Grisham** 

Re: Incoming-call identification

**Brint Cooper** 

Risks of telephone access to your bank account

**Brint Cooper** 

Limitless ATMs

Emily H. Lonsford

Re: A Touching Faith in Technology

**Henry Spencer** 

Risks of helpfulness

**Henry Spencer** 

Work monitoring survey

Goun

Faking Internet mail

Robert C. Lehman

Spying on or intercepting UUCP mail

**David Sherman** 

Hackers, cartoons, and computers

**Doug Claar** 

Info on RISKS (comp.risks)

### **✗** Re: Sunspots & Communications

Jordan Brown <herron!jbrown@jato.Jpl.Nasa.Gov> Fri, 17 Mar 89 10:09:13 PDT

#### PGN writes:

> In the Mount Diablo area of California, there have been many reports of

> garage door openers failing to operate.

KFWB reported that this was caused by some form of radio transmitter that the Navy was using in the area (paraphrased) "to provide communications to a ship at Alameda while its communications gear was being repaired". It's been turned off. The report was technically quite vague, so I can't provide more detail.

Jordan Brown [Also noted by Barry Klawans and Steve Wilson]

[The old joke used to be "When is a door not a door?" "When it is ajar." Now we have a new joke, "When is a door not a door?" "When it is ajam(b)." PGN]

### **✗** Re: Sunspots & Communications

<Gasbarro.pa@Xerox.COM> 16 Mar 89 17:26:07 PST

- > I thought that [garage door] openers operated in the microwave range;
- > isn't this power level of transmission unhealthy?

Most garage door openers that I've encountered operate in the 380MHz range. Water resonates at 2.4GHz. Besides, the power level is only a few tens of milliwatts.

### Ethics of Copying Fonts

jss@ulysses.UUCP <Jerry Schwarz> Fri, 17 Mar 89 11:02:24 EST

Marc Mengel ... exactly illustrates why this is a gray area. Suppose that they didn't pick out the letters but were distributing the whole page? Cleary a violation of copyright. Individual columns? Still a clear violation. Individual pixels? Clearly permitted, but only because they used no NYT information content. Why bother digitizing the NYT to get bits in simple patterns when you can generate them yourself? Somewhere in between (around the word or letter level) lies a gray area.

My (moral) conclusion is that if its worth copying something then there is value in whats being copyied. If the value derives from effort that is not required to make the copy then there ought to be a way to protect that effort.

Jerry Schwarz

# Policy Statement Request

Dave `White Water' Grisham <dave@charon.unm.edu> Fri, 17 Mar 89 10:52:44 MST I am currently (re)writing our Univ. policy on "computer misuse". Rather than reinvent the wheel, I ask anyone who has access to an enforceable, yet comprehensive policy statement to please share it with me. My research to date has shown many universities to be behind in their written-published policies. I believe courts will find that policies written before networking and viruses are of little value. I will be glad to post the results of my efforts individually or to the group. Thanks in advance. dave

Dave Grisham

Senior Staff Consultant/Virus Security Phone (505) 277-8148
Information Resource Center USENET DAVE@UNMA.UNM.EDU
Computer & Information Resources & Technology BITNET DAVE@UNMB
University of New Mexico Albuquerque, New Mexico 87131

### Re: Incoming-call identification

Brint Cooper <abc@BRL.MIL> Thu, 16 Mar 89 9:24:50 EST

Incoming-call ID is a difficult problem. Still, doesn't a person, in the privacy of Home, have the right to an "electronic peep-hole" to control his/her privacy?

This is a larger issue than screening out the vendors who call at dinnertime. The police and telecos simply are ineffective at dealing with persistent, harrasing and/or obscene callers. Their methods are cumbersome and non-responsive to the harrassment.

Any caller can protect his/her privacy by calling from a work phone (which is a very common practice, prohibitions notwithstanding) or from a pay phone.

Incidentally, what is the "scope" of Incoming Call-ID? Does it identify only calls from the same central office? local calling area? area code? or country? A function similar to Incoming Call-ID is how our teleco gathers "evidence" on harrassing phone calls. The harrassed plaintiff keeps a date/time log of objectionable calls; the teleco may be able to tell the originating phone number. However, in our case, it could resolve only phone numbers in the same central office as the harrassee and, perhaps, a small number of other, specified, central offices.

I'm a firm believer in privacy, too. But that includes my right to privacy in my own home.

\_Brint

### Risks of telephone access to your bank account

Brint Cooper <abc@BRL.MIL> Thu, 16 Mar 89 9:29:31 EST

In discussing "Risks of telephone access to your bank account," Michael McClary relates the identifying information required to transfer funds

by telephone, then observes:

- > Now combine that with cellular phones that:
- > are not scrambled,
- > don't switch channels enough to break up a conversation,
- > can be rec[ei]ved on the high end of an old TV set's UHF dial
- > are generally owned by busy people with money
- > and you've got the makings of some nasty surprises.

Get the word out, folks: CELLULAR PHONE IS NOT "TELEPHONE." IT'S BROADCAST RADIO! DON'T SAY ANYTHING ON CELLULAR PHONE THAT YOU WOULDN'T SAY ON YOUR LOCAL RADIO STATION!

Brint

# ✓ Limitless ATMs (Re: RISKS DIGEST 8.37)

Emily H. Lonsford <m19940@mwvm.mitre.org> Friday, 17 Mar 1989 17:02:51 EST

Some years back, when ATMs were first coming out, I signed up for a card at my bank. The first time I used it was a memorable experience. The machine was very primitive. Instead of a CRT, it had colored buttons with messages like "Insert card" or "Enter your PIN" which were illuminated to instruct the user. I dutifully inserted my card and followed the instructions. "Clickety click!" responded the machine, and then told me to enter my PIN. After each action on my part, there was a noticeable pause and more "clickety clicks" from the machine. I soon decided that the clicks were there to keep me, the poor dumb user, occupied while the machine communicated with the host. This struck me as terribly funny, and I began to chuckle. Each set of clicks made me laugh harder, and people were beginning to stare. The best part was yet to come: when the machine finally spit out the money, it was crisp and new - and WARM, as if it had just been printed! It was all I could do not to roll around on the floor laughing; I grabbed the money and my card and left.

A couple of years later, one of the bank's systems programmers explained the machines to me. "Oh," he said very seriously, "the clicks really had a purpose. The machine had no link to the bank; instead it had a ticker tape inside, and it recorded every transaction (hence the clicks.) A technician came around every day, collected the tape (which was keyed into the bank's main computer) and refreshed the money supply." And as for the crisp new bills? "Well, those machines were so cantankerous that they would jam if anything but new money was used."

As usual, there was a logical reason for everything the computer did. I think I liked my interpretation better.

The moral is, these machines were vulnerable to the kind of attack mentioned in RISKS 8.37. They depended on the cooperation of the user not to go around and collect \$300 from each machine. Security via ignorance....

Emily H. Lonsford, MITRE Houston W123 (713) 333-0922

### Re: A Touching Faith in Technology

<henry@utzoo.UUCP>
Fri, 10 Mar 89 16:08:28 -0500

>"The adoption of an identity card, at least on a voluntary basis, which would >carry such numbers - name, date of birth, nationality, signature and perhaps >blood group - would surely be an advantage for everybody...

Of course, "voluntary" is likely to mean "compulsory" very quickly, unless this is specifically illegal. I have neither an age-of-majority card (the only legal proof of drinking age here) nor a driver's licence, and you'd be surprised at the looks this sometimes gets me.

Blood group, eh? How soon before AIDS-test status gets included?

>... GIVEN THAT TECHNOLOGY SHOULD MAKE IT IMPOSSIBLE TO FORGE THEM, >such cards could quickly establish one's bona fide. . . ."

This runs into the same problem that (I understand) Germany ran into after WW2. There were many people with little or no identification in the chaos that followed Germany's defeat. Some of them were wanted men. There was felt to be a need for one solid form of ID, something sufficiently well-researched to be definitive. The obvious choice was the passport. What this meant, in practice, was that if one could get a forged passport (not easy, but not impossible), nobody would ever question one's new identity.

Henry Spencer at U of Toronto Zoology

### Risks of helpfulness

<henry@utzoo.UUCP>
Fri, 10 Mar 89 15:49:27 -0500

I haven't seen this one mentioned here yet... At the San Diego Usenix conference at the beginning of last month, in his keynote speech, William T. O'Shea (VP of AT&T) said that twice recently, intruders got into AT&T systems by being talked through the sign-on procedures by AT&T help desks!

Henry Spencer at U of Toronto Zoology

### Work monitoring survey

<goun%evetpu.DEC@decwrl.dec.com>
10 Mar 89 09:47

From The Boston Globe, Thursday, March 9, 1989:

Most workers in survey think employers use electronic means to spy on them

By Ronald Rosenberg, Globe Staff

A survey said that 75 percent of mostly unionized workers in Greater Boston feel ``spied on at their jobs'' by electronic monitoring.

The survey, conducted by the Massachusetts Coalition on new Office Technology, which represents over 40 unions and women's organizations, has filed state legislation that would require notifying employees in advance of any monitoring or surveillance. A legislative hearing on the measure is scheduled Monday at the State House.

Several insurance firms, banks, airlines and industry groups oppose the legislation, saying it is unnecessary and violates an employer's right to monitor how employees work.

At issue is the use of computerized or electronic monitoring systems to keep track of an employee's work performance and activities. This kind of surveillance includes computer monitoring where the computer counts keystrokes, error rate, time to complete each task and break time.

Another way checking [sic] on employee productivity is service observation where supervisors listen into conversations between employees and customers.

A third form, known as telephone call accounting, monitors the time, length and destination of all calls dialed from each extension but does not record the conversation. It is used by telemarketing firms and large sales organizations.

"There have been clear abuses of electronic monitoring and it violates a person's right of privacy and right of due process," said Lisa Gallatin, the coalition's executive director.

# Faking Internet mail

Robert C. Lehman <rcl@jolt.cc.columbia.edu> Tue, 14 Mar 89 14:54:23 EST

While "faking" electronic mail may be easy, it's not as easy as faking "physical" mail. More specifically, getting some company or university letterhead (or having some printed, for that matter) and typing up a letter requires less specific knowledge than hacking some system's SMTP mailer, for example.

However, people perceive computers as being reasonably secure entities, and therefore they assume that electronic mail generated by a computer system is genuine.

While an organization such as NSF, which is accepting reviews of proposals via electronic mail, should be concerned about the authenticity of reviews it receives, reviews sent by electronic mail are, in the long run, no more or less likely to be bogus than those sent by surface mail.

Robert Lehman, Columbia University

# Spying on or intercepting UUCP mail

David Sherman <dave@lsuc.uucp> Wed, 8 Mar 89 23:51:24 EST

Peter Scott (pjs@grouch.jpl.nasa.gov) writes in RISKS 8.28:

- > > Walter Roberson in RISKS-8.27
- >>How about the
- >>other way around: how much danger is there that someone can spoof mail in
- > >order to receive messages destined for someone else?

>

- > The only way I know of doing this is if your machine is on the path for
- > the mail in the first place, in which case you can look at everything
- > that passes through anyway.

All it takes is a published "mysite uunet(LOCAL), att(LOCAL)". Now that most sites on the net use automated routing with pathalias, a sysadmin with long-term general spying goals need only show very fast connections to major sites in the system's official UUCP map entries. Within a few months a lot of mail from nearby sites will be coming through. Keeping a copy of everything that passes through is as trivial as setting a #define in smail.

David Sherman, The Law Society of Upper Canada (att!lsuc!dave :-))

### Hackers, cartoons, and computers

Doug Claar <dclaar%hpda@hp-sde.sde.hp.com> Mon, 13 Mar 89 17:32:44 pst

Recently, while watching my kids watch Saturday cartoons, I noticed a "Computer Minute" public service type add from the network. In it, the father, who was portrayed as clueless, was trying to organize his towering stack of papers. His son, Hacker, tried to tell dad all about Data Base Management Systems. Why, even sister had her (girl stuff) on the computer, and gee, mom had her recipies. Hacker had his (boy stuff) on it as well. Having only seen one, I don't know for certain, but given the girl's name (which I don't remember, but wasn't computer-oriented), and the son's name, it seemed to perpetuate the young male as the hacker stereotype.

Relationship to risks? Well, I've seen discussions on the term "hacker," and on comics and computing.

Doug Claar, HP Computer Systems Division
UUCP: mcvax!decvax!hplabs!hpda!dclaar -or- ucbvax!hpda!dclaar



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 8: Issue 41

# Monday 20 March 1989

# **Contents**

20+ year, \$100+ million Army software project

Jon Jacky

Formal methods to be applied in Australian railroad switching Jon Jacky

Error in updating new specifications for call-routing Pertti Jarvinen

Risks of Registering Shareware

A. Lester Buck

Risks of helpfulness

Jerome H Saltzer

Remote Smart-Cards

lan W Moor

Re: so-called multi-gigabuck theft of information

**Mark Brader** 

Re: NASA to replace top-level personnel with Expert Systems Robert English

Meter Readers an Endangered Species?

David K. Black

Security of Electronic Mail

Karl Lehenbauer

Star Trek computer virus

Colin P.

Info on RISKS (comp.risks)

# ✓ 20+ year, \$100+ million Army software project

Jon Jacky <jon@june.cs.washington.edu> Fri, 17 Mar 89 17:15:06 PST

In view of all the postings a while back about runaway software projects, I found very interesting these excerpts from GOVERNMENT COMPUTER NEWS, Feb. 20, 1989, p. 59:

ARMY TO CONVERT 'CENTRAL NERVOUS SYSTEM' TO ADA by Karen D. Schwarz

The Army issued a request for information last month to convert its All Source Analysis System (ASAS) to Ada code. ... ASAS is being developed by the Joint Tactical Fusion Program Management Office (JTFPMO) on behalf of the Army and the Air Force. It has been in development for more than 10 years. ...

More than 800,000 lines of code have been written in FORTRAN 77 so far. The project is expected to begin using Ada code in fiscal 1991. By that time, more than 1 million lines of FORTRAN 77 code also will have been written.

A document detailing JTFMPO's major programs refers to ASAS as the "central nervous system" guiding field commanders in battle. ASAS is a key component of the Army Command and Control System and will automate command and control of intelligence/electronic warfare operations. ASAS will fuse raw battlefield data into intelligence for analysis on a workstation. The services can then distribute resulting information to battlefield commanders, fire support elements and the Air Force to help control electronic warfare equipment. ...

The project is scheduled to be completed sometime after the year 2000. Although he would not estimate the total costs of the program, deputy for plans and integration at JTFPMO Bennet Hart said software costs alone might exceed \$100 million over the life of the contract. ...

The JTFPMO has received many replies to the request for information, Hart said. "Response from industry has been very good. No one is conspicuous by their absence."

The Jet Propulsion Laboratory (JPL) in Pasadena, Calif., currently holds a contract for the first phase of the project.

- Jonathan Jacky, University of Washington

### Formal methods to be applied in Australian railroad switching

<JON.JACKY@GAFFER.RAD.WASHINGTON.EDU>
17 Mar 1989 16:49:02 EST

Here are excerpts from ELECTRONICS ENGINEERING TIMES, Feb. 20 1989, p. 28:

High-integrity uP wins first big order: Railroad signals go-ahead for Viper by Roger Woolnough

Worcester, England --- In the first significant order for the chip, the Australian National Railways Commission has placed a contract for signaling systems incorporating Viper to control two long-distance rail routes. ...

Viper is a 32-bit RISC device designed to overcome the shortcomings of conventional microprocessors, which can be unreliable in safety-critical applications because they can perform in unpredictable ways. The design of Viper was undertaken using formal mathematical methods and was then

subjected to a series of formal proofs to ensure that the implementation conforms to the design specification. ...

In Australia, the contract to develop and supply railroad signaling equipment using Viper was won by Teknis Systems (Australia) Pty. Ltd. Support was provided by Charter Technologies Ltd. (the British Viper specialist), and the two companies believe that proposing Viper as the system processor was a major factor in Teknis being chosen against strong competition.

The contract is to design and supply signaling for automatic crossing sections on the Trans Australian and the Central Australian rail routes, operated by the Australian National Railways Commission, a federal government statutory authority. ...

The installations will include trackside equipment, systems on board trains, radio links and a computer-controlled center in Adelaide. ...

Formal methods will be used throughout the development. ... Charter Technologies is sponsoring a study by the Department of Engineering in the University of Warwick, England, into the use of formal methods for railroad signalling. ...

Railroad signalling systems around the world are based on concepts of interlocking and routing which have developed over the past 150 years. The first-class safety record of railroads is due to a large extent to the rigor of the regulations.

The aim of the joint study by Charter Technologies and Warwick University is to consider whether the well-established rules can be formulated in a mathematical way, so as to suit the increasing use of computer-controlled interlocking and routing. ... It will consider the application of the specification language HOL developed at the University of Cambridge, England; programming in subsets of computer languages such as Pascal; and the use of Viper. ...

- Jonathan Jacky, University of Washington

### Error in updating new specifications for call-routing

from Pertti Jarvinen, Finland Mon, 20 Mar 89 08:43:56 +0200

The Finnish Post and Telepohone office was March 6 changing call-routing specifications in one of three main computer-controlled switches at Helsinki, the capital of Finland. Some of necessary changes was forgotten. To this end traffic via the switch was broken for two hours. The error was located and corrected in six hours. Domestic calls were turned to go via two correctly functioning switches. But some international calls, for example, to Canada, Portugal, Iran, Turkey and Cyprus were totally hindered.

As a remedy to prevent similar errors in the future systems analysts propose a programmed checking for implementation of all the necessary changes.

### Risks of Registering Shareware

<@sri-unix.UUCP, @rutgers, @texbell, buck%siswat@moray> Wed, 8 Mar 89 03:38:55 EST

I just sat through a user's group demo of a new shareware package called BackMail, which is a background electronic mail package for MS-DOS. It is a slick program with many fine features for supporting local and long-distance mail networks. The authors were leery of the standard shareware registration procedure. Quoting from the BackMail Newsletter:

"The problem was that the whole process of payment was so cumbersome. If only there was a simple way to communicate one's payment... Hold it! Communication is just what BackMail was about. We had the first program that could be used to \_literally\_ pay for itself! And so TeleWare was born."

Yes, your copy of BackMail is registered by filling in a screen with your credit card information and the program automatically calls an 800 number to deliver the information. And most users will register (\$30), since BackMail asks you to register on every fourth access of the program's main functions, and complains for twenty seconds if you don't register.

The risks of this scheme for freely redistributable shareware are obvious, from simply patching the stored 800 number to saving the credit card information and making one "extra call" at the program's convenience.

A. Lester Buck ...!texbell!moray!siswat!buck

### Risks of helpfulness (RISKS-8.40)

Jerome H Saltzer <jhs%computer-lab.cambridge.ac.uk@NSS.Cs.Ucl.AC.UK> Mon, 20 Mar 89 11:03:05 gmt

- > intrudesr got into AT&T systems by being talked through the sign-on > procedures by AT&T help desks!
- > Henry Spencer at U of Toronto Zoology

The specific incident may not have been mentioned in RISKS, but the general technique is widely enough known that it is casually mentioned in the hacker periodicals (such as the magazine "2600") when they run an article of tips for beginners. If you are having trouble getting into someone's system, call up their consulting office and act like you are authorized but encountering unexpected trouble logging in; often someone there will give you just the clues you need.

Jerry Saltzer

#### Remote Smart-Cards

<iwm@doc.imperial.ac.uk>
Mon, 20 Mar 89 04:17:24 PST

#### Backround:

A bill to require all major football (Soccer) grounds in the UK to require a valid machine readable membership card before admitting a spectator is currently going through Parliament. The clubs will be given lists of people who should not be admitted; the object is to stop violence in the grounds.

Several objections have been raised -

Civil Liberties:

People object to having to carry the cards, and to having football clubs provided with information about them.

Practicalities:

The card readers, turnstiles, or the computer controlling them may fail, leaving thousands of angry fans outside.

Last month New Scientist carried an item describing a proposed solution, remotely readable and writeable smart-cards. (In this case the card has to be writeable to prevent it being passed over the fence and used again.) The cards are made by Plessey and the read/write range is quoted as about a meter; power is taken from the signal.

Consider the risks: the card can be read (AND WRITTEN) without you knowing and without your control. Obviously the card could check that it was being interrogated by a legal reader using some kind of validation (public key challenge and response?) but there will be a limit to how much processing the card can do and as the reader has to broadcast to activate the card, it may be very easy to record a dialog and spoof either the card or reader.

Ian W Moor, Department of Computing, Imperial College, 180 Queensgate, London SW7 UK UUCP: uunet!mcvax!ukc!icdoc!iwm JANET: iwm@uk.ac.ic.doc

# ★ Re: so-called multi-gigabuck theft of information (RISKS-8.23 ff.)

Mark Brader <msb@sq.sq.com> Fri, 17 Mar 89 16:43:13 EST

- > From msb Fri Feb 24 06:40:01 1989
- > To: utzoo!attcan!uunet!csl.sri.com!risks
- > Subject: Re: so-called multi-gigabuck theft of information
- > Bcc: hcr!mike

There appeared in Risks 8.23 my summary of a newspaper item I'd noticed about what was said to be a "theft" of highly valuable computer data. A followup newspaper article, which I summarized in Risks 8.28, provided a good deal more information and placed a much lower value on the data, but while it identified the victim (HCR Corp., of Toronto), it did not identify the "stolen" data.

So I was surprised to see Jeff Makey assert in 8.26, which I read after submitting my second item, that what was taken was a copy of the UNIX source. I emailed him and he replied in part:

> I heard it \*somewhere\* during the last few months (it seems like > it was before Christmas, which is why I said it wasn't news).

Since the HCR case was much more recent, Jeff had to be talking about a different one. In fact, with that hint I remember the one he had in mind; the confusing thing is that it happened to also have occurred in the same geographical area. (Toronto: Canadian computer crime capital?)

The earlier case hasn't been mentioned in Risks before. [???] What happened, as I recall, was that someone bought a used computer at auction, found a copy of the UNIX source on its disks, and claimed all rights (!) to use the source, thus making the newspapers. AT&T of course disagreed, and I believe the case dropped out of the news before it was resolved.

Someone I was chatting about this with conjectured that the \$4 billion (Canadian) valuation that appeared in the first newspaper article might have resulted from a reporter also confusing the two cases and assuming that because HCR has UNIX source then that must be the valuable thing in question, and then taking the highest possible valuation. Such a speculation would also explain why the second article suddenly started talking about AT&T, which had not been mentioned in connection with the case. Simple press speculation/sensationalism.

Of course, there's more than one way to value copyable things like computer programs or data. It's correct to say that the UNIX source is worth kilobucks because you can buy a copy for your own use for that much. It's also correct to say that it's worth gigabucks, if that's how much money AT&T earns from it over the lifespan of the system. In addition, one must distinguish between theft and illegal copying. The former, I think, would be better defined as involving loss to the owner of one or more copies of the original. (Of course, the newspapers prefer to use the more dramatic word.) Anyway, if ALL copies were stolen in this sense, then the value of the loss to the owner suddenly becomes much greater.

Also since submitting to Risks the second newspaper article, I have spoken to Mike Tilson, president of HCR, who was quoted in it. He confirmed that the first article was "wildly inaccurate" and the second one was substantially, though not entirely, correct. (He noted that Risks readers ought to be aware of the risks of believing what they read in the paper...) He also confirmed that HCR was not saying what was taken, only that they had regained complete control of it.

So I think that wraps up this case as far as Risks is concerned.

Mark Brader utzoo!sq!msb msb@sq.com

★ Re: NASA to replace top-level personnel with Expert Systems

Robert English <renglish%hpda@hp-sde.sde.hp.com> Mon, 20 Mar 89 11:19:06 pst

An AI friend of mine told me recently that most expert systems have a relatively short useful lifespan. It seems that if you assign a human to operate the system, the human will soon stop using the ES, and do a better, faster job without it. The ES makes an excellent training system, however, and creating it does a good job of recording what the job entails, information which is often lost when people change jobs.

--bob-- renglish%hpda@sde.hp.com

### Meter Readers an Endangered Species?

<black%par1@cs.umass.edu>
Mon, 20 Mar 89 16:26:03 est

The following appeared in the March 13 Wall Street Journal:

**Human Meter Readers Step Toward Extinction** 

Meter readers' jobs are being threatened by technology.

Boston Gas Co. recently became the firsr utility in the country to commit itself to installing a radio-based automated meter-reading system for all its customers. It plans to install the AccuRead system, made by Enscan Inc. of Minneapolis, in some 400,000 homes at a cost of over \$20 million. The system will eliminate most of the utility's 100 meter readers who make an average of \$28,000 a year.

The AccuRead system ... uses a cigarette-pack-sized radio receiver and transmitter that is attached to the gas meter. The device counts the number of times the dials spin. Once a month, a computer-equipped van cruises the streets nearby and sends out a "wake-up" signal to the reader device, which then transmits the gas consumption. the devices have 10-year batteries and a 32 year meantime between failures, Enscan says.

Boston Gas says the remote readings have a number of pluses. Homeowners don't have to be in for readings; unlike humans, THE DEVICES DON'T MAKE MISTAKES, and the information can be sent automatically from the van to the billing computer without retyping.

Moreover, says a spokesman: " It will elimimate estimated bills which are the biggest complaint we have...."

....no doubt the devices are as reliable as the average garage door opener.

David K. Black Umass Amherst

### Security of Electronic Mail

Karl Lehenbauer <karl@sugar.hackercorp.com> 19 Mar 89 18:08:29 GMT

While "everybody knows" or should know that electronic mail is not secure in that its contents can be read en route, the reason people generally trust their email as being authentic is because it usually is; that is, there has been very little email forgery hence it hasn't been much of a problem, thus people tend to regard their email as being genuine. When it starts to become a problem, people will stop trusting it, at least when it's important.

It seems that faking comments on a grant proposal would be prosecutable as fraud.

As for security from interception, a DES encryption program that is free of U.S. export controls (as it was written and distributed from outside the country) was recently posted to one of the Usenet source groups. By using this and something like uuencode (a common program on Usenet that reversibly maps unprintable characters to printable ones) on one's text, one can keep their mail private from the prying eyes of most individuals.

The security of one's electronic mail from decryption by the National Security Agency is a different matter, and one that I hope is merely academic to most RISKS readers. As to whether or not they can relatively easily decrypt DES-encoded material, let me say that I would not expect such a group to widely promote an encryption scheme that they were incapable of breaking and that, from a national security standpoint, doing so would not be such a good idea.

Within the Internet, it is my understanding that the steering committee has endorsed the RSA encryption scheme for email. This addresses both the privacy and forgery issues. I think we will see further movement toward routine encryption of email, and it is high time that we do so.

Cellular phone data encryption is a relatively simple matter as well. I don't think we'll see any movement in that area until the users demand it, and the government isn't likely to push heavily for it, a few strong proponents of personal privacy in the legislature nonwithstanding.

### Star Trek computer virus

<microsoft!w-colinp@uunet.UU.NET>
Sun Mar 19 22:05:13 1989

This (including threats to take over the ship) has already happened on Star Trek: The Next Generation. Data was playing Sherlock Holmes in a computer-generated simulacrum, but since he had memorised all existing Holmes plots, the computer was asked to come up with a new one, involving an enemy "capable of defeating Data." Because Data, unlike Holmes, lives in the "real" world, this one-word slip produced an opponent also capable of affecting the "real" world, which attempted to take over the ship.

It was portrayed more as a question of sentience (the conclusion was that

the created personality was stored until technically feasible to give it corporeal existence), but we had a computer program, in this case inadvertantly created (grave RISK indeed!), attempting to control the ship.

I suspect that treating the problem directly, the writres will massacre the issues. But I may just be overly pessimistic.

-Colin (uunet!microsoft!w-colinp)



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 8: Issue 42

# Monday 20 March 1989

# **Contents**

Automatic Caller Identification

Phil R. Karn

Robert Goldman

John Murray

Bernie Cosell

Karl Lehenbauer

Dean Riddlebarger

**Mark Mandel** 

Phil R. Karn again

Benjamin Ellsworth

more or less chronologically

Info on RISKS (comp.risks)

# ✓ Internet spoofing and Calling-party ID (Re: RISKS-8.38)

Phil R. Karn <karn@thumper.bellcore.com> Fri, 17 Mar 89 22:11:13 est

I hope I am not the only one to notice the irony in the parallel discussions regarding, on the one hand, concern about the possibility of spoofing source addresses in Internet mail (most often done in practice to gain anonymity), and other hand, privacy concerns about calling party identification in the telephone network.

Two things seem clear to me.

- 1. As a telephone subscriber, I should have the right to demand identification from anyone ringing my phone.
- 2. As a telephone subscriber, I should have the right to remain anonymous when making a call if I so choose.

The obvious solution to these conflicting requirements is to have the telephone system arbitrate a negotiation between the caller and called parties. If a caller wishes to remain anonymous, he should be able to say so when he dials his call. If the called party has chosen to demand identification, then the network should refuse to complete the call and explain why to the caller -- without ringing the called party's phone.

If the calling party has not requested anonymity, there is no reason to deny the called party this information. I see no reason to condemn a promising new service like Caller ID when a relatively simple enhancement could satisfy the privacy concerns of both parties.

(This is my personal view, and is not necessarily the view of my employer). Phil

# Incoming-call id

Robert Goldman <rpg@cs.brown.edu> Fri, 17 Mar 89 22:32:52 EST

I think Brint Cooper underestimates the technological possibilities when he(?) writes:

Incoming-call ID is a difficult problem. Still, doesn't a person, in the privacy of Home, have the right to an "electronic peep-hole" to control his/her privacy?

We can have our cake and eat it, too. As I understand it, it is possible to have the originating caller notified of the ID process, and given the opportunity of aborting the call rather than being identified. BUT only if your local phone company gets enough requests for this service.

This seems like the ideal compromise: you have to be willing to be identified to reach someone, but you are informed that they are tracing you, and can deny them that service.

The source for this was a WSJ article. I'm afraid I've forgotten the exact citation. If anyone has it, it would probably be of interest to all the list: it discussed which phone servers were going to provide the incoming-call ID service, and which were and weren't going to install the out I've mentioned above.

# Re. Incoming-call identification

John Murray <johnm@uts.amdahl.com> 17 Mar 89 20:33:02 GMT

The discussion on the pros and cons of incoming-call identification reminds me of the Confidential Phone service in Northern Ireland. By calling a widely-advertised number, people in Northern Ireland can use an answering machine to report information about terrorist activity to the police/army. The line is supposedly unmonitored, not traced, and completely confidential.

Some years ago, a popular pastime for bored teenagers was to call the number from a public phone and start to record some juicy information. They would then make a noise as if they'd just been stabbed or attacked in some way, and hang up. It would come as no surprise when a police or army patrol arrived on the scene within a minute or two. Naturally, the patrol could do nothing, since any action on their part would expose the "confidential" nature of the system!

- John Murray, Amdahl Corp. (My own opinions, etc.)

# Re: Incoming-call identification

Bernie Cosell <cosell@WILMA.BBN.COM> Sat, 18 Mar 89 17:57:59 EST

I truly hesitate to bring the ANI-wars to risks (they're already a couple of weeks old on telecom now), but ... First, this argument is VERY common in this debate and strikes me as fundamentally off the mark:

- > Incoming-call ID is a difficult problem. Still, doesn't a person, in the
- > privacy of Home, have the right to an "electronic peep-hole" to control
- > his/her privacy?

Without going into this at length, I'll just assert that the \*correct\* parallel here should be the use of an answering machine to screen your calls. The answering machine does EVERYTHING the peephole does and more (it allows you the privacy of having the person-you're-screening not even KNOW if you're there doing the screening or not: like simultaneously having a closed-circuit-TV (which doesn't let the caller know if you're looking at the monitor or not) \*with\* an old-style "chain" that lets you open the door a crack and ask the person who the hell they are and give them an opportunity to explain what they're up to, while STILL denying them access to your house. ANI has nothing to do with any of this, and by contrast, just a "peephole" is a lot closer to just answering the phone (the doorbell rings, you have to go to the door, open the peephole, and choose whether to go farther or not, not much different than answering the phone and hanging up).

- > This is a larger issue than screening out the vendors who call at dinnertime.
- > The police and telecos simply are ineffective at dealing with persistent,
- > harrasing and/or obscene callers. Their methods are cumbersome and
- > non-responsive to the harrassment.

You made a leap from "privacy" to "harrassment" here. You can have more than adequate (IMHO) protection from "harrassment" just by having \*telco\* use the ANI machinery on your behalf [as has been suggested: telco keeps the information about calling parties and releases it ONLY to folks with a "need to know"].

Bernie Cosell, BBN Sys & Tech, Cambridge, MA 02238

# Re: Incoming-call identification, phone number is not enough

Karl Lehenbauer <karl@sugar.hackercorp.com> 19 Mar 89 17:01:43 GMT

Regarding incoming-call identification, for this to be usable by most people, different information than the phone number of the caller must be sent. Specifically, some kind of logical ID should be at least included, or sent in place of, a physical ID.

Consider that if one was restricting incoming calls to a specific set of numbers, one could not receive an emergency call from a loved one. Few families would be willing to take this risk, so one the good aspects of incoming-call identification, screening calls, would be lost to them. For incoming call screening to be useful in this case, one would have to forward a logical ID. "This is a call from your daughter" rather than "This is a call from (713) 438-5018."

Similarly, phone solicitors would be required to forward a special ID indicating that they were calling you with an unsolicited sales pitch. Thus they could be explicitly excluded. I think there should be a bit in the header to indicate whether the call was being handled entirely by automatic equipment as many people (myself included) find those calls particularly offensive and choice targets for elimination.

The ID would be sent by entering additional digits or by using something like a credit card with a magnetic stripe. One must already identify oneself by one of these methods when using long distance carriers from remote phones. Cellular phones already identify themselves uniquely as well.

Note that similar capabilities are already available in certain high-end answering machines and corporate voice mail systems whereby one can give IDs out to people and dispatch calls based on the IDs entered.

To the extent that incoming-number forwarding increases privacy (and implicitly, honesty) I think it is a good thing. To the extent that it decreases privacy (use of it to catch whistle blowers, perform arbitrary surveillance, etc), I think it is a bad thing. Simply forwarding the telephone number of the caller does little to advance the privacy of the individual and is of more use to business and government, would would have the resources to look up the number and determine the True Name of the caller, on-line.

Karl Lehenbauer

### Incoming Call ID (Re: RISKS-8.40)

Dean Riddlebarger <rdr@killer.dallas.tx.us> Mon, 20 Mar 89 06:31 CST

In the last issue of Risks, one of the contributors wondered about the mechanics of Incoming Call ID. Now, from what I have seen in my intracompany readings, Incoming Call ID in its most basic form is just a pass through of

standard Central Office ANI functionality, so it would be capable of handing a complete number of format NPA-NXX-XXXX to the user.

I'm still not sure I fully understand the dynamics of this latest uproar. The capability of number ID has been widely touted as a major initial feature of ISDN for several years now, so I find it interesting that when a telco moves the notion from business applications to a more home-oriented use the proverbial balloon finally goes up...

Dean Riddlebarger, Systems Consultant - AT&T, [216] 348-6863

### Re: Incoming-call ID

Mark Mandel <Mandel@BCO-MULTICS.HBI.HONEYWELL.COM> Mon, 20 Mar 89 10:16 EST

I agree with Brint Cooper in support of incoming-call ID. Our area will be getting this service in a few months, and we intend to order it and buy the \$60-70 gadget. Why? We have a peculiar, repetitive telephone number, with the pattern XYY-ZZZZ (we didn't ask for it: telco assigned it to us), and we get a large number of unwanted calls in the following categories:

- 1: "Stutter" wrong numbers. Somebody wants XYY-ZZZA, ZZAB, or ZABC, and either the finger stutters on the Touch-Tone pad or the pad stutters; one or more extra Z's are generated, the extra digits get thrown away, and they reach me. Sometimes they're polite ("Oh, I'm sorry"), sometimes they're rude.
- 2: Crank callers. For reasons I omit here, our number attracts even more cranks than you would expect from what I've stated here.
- 3: Prank callers. I refer here to the deliberate nuisance calls that come from my daughter's seventh-grade classmates being seventh-graders.
- 4: "Not her father!" calls. A classmate calls my daughter, hears my voice (or my wife's), and instead of asking for my daughter simply hangs up without saying anything.
- 5: Business wrong numbers. The same XYY-ZZZZ number evidently belongs to at least two commercial accounts: in different area codes, of course, but one of those area codes is the next one over, and another differs from ours in only one digit. I know because we've been getting responses to their newspaper ads.
- 6: Oh, I almost forgot: random wrong numbers, the same kind as anybody else gets incoming.

I think that covers it. Now, incoming call-id won't affect all these categories, but it WILL give us a tool to use against types 2, 3, and 4. If we didn't have the peculiar problems raised by our particular number, I don't know if we'd bother (though 4, and probably 3, would still be there); but the total volume of wrong numbers is enough to make us willing to put in the money and effort to achieve the reduction we expect to get.

-- Mark Mandel

<sup>\*</sup> My employer is not responsible for anything I say, think, do, or eat. \*

### Re: Incoming-call identification

Phil R. Karn <karn@thumper.bellcore.com> Mon, 20 Mar 89 13:41:23 EST

Caller-ID recently became available in my exchange in Northern New Jersey (area code 201). I asked the customer service rep about the coverage of this service. The answer, somewhat reluctantly divulged after a bit of prodding, is that the display works only for calls from other phones in the 201 region, and then only those phones on "suitably equipped" exchanges (presumably the right kind of ESS's).

This seemed a bit restrictive for a \$6/mo service, so I've decided to wait. Phil

# Confidentiality of incoming numbers (Re: RISKS-8.38)

Benjamin Ellsworth <ben%hpcvlx@hp-sde.sde.hp.com> Thu, 16 Mar 89 17:01:27 pst

I find myself in hearty disagreement to David Albert's stridently stated position. This disagreement stems from my opinions about anonymity. The anonymity that he seems to be promoting/preserving -- the ability to initiate and carry on a dialog with either or both parties ignorant of the identities of the other -- very new social concept. Even in its current form, it is illusory at best.

As little as 100 years ago in this country (and currently in much of the world) in order to talk to someone you have to be in fairly close physical proximity. This fact makes anonymity almost impossible. It is not a grave flaw in societies where this is the case.

It should be pointed out that in societies where "anonymity" is not technically ensured, it is ensured by trust. Even now in our society, the real assurance that no one will find out who you are is that no one will look. (In most modern phone networks your veil of anonymity is tissue paper.) For all of the institutions that David feels are threatened by technology, trust will suffice. If any of those institutions violates that trust, it will find itself unused. If unused, unfunded. Either the service proves itself worthy of trust or it disappears.

Where's the RISK? Looking for and believing in hardware solutions to purely "wetware" problems. If trust is the problem, it must be fixed in people (their attitudes and organizations) not in their appliances. Machines may make humankind more powerful but machines do not make them more trustworthy.

BTW - I will take David's advice and write to the people he mentions. I will write in support of the concept that, on my discretion, to talk to me you must surrender your anonymity.

Benjamin Ellsworth, Hewlett-Packard, 1000 N.E. Circle, Corvallis, OR 97330



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 8: Issue 43

Tuesday 21 March 1989

# **Contents**

Outdated codes made US missiles useless

**Henry Cox** 

Risks of dving batteries

**Henry Cox** 

Things to do with a computer...

Joe Morris

Possible Cancer Risks from Cellular Phones?

Mike Trout

Supreme Court and Copyrights

ark

Mitnick plea bargain

**Rodney Hoffman** 

Re: Risks of telephone access to your bank account

Phil R. Karn

Internet Security Plans

Vin McLellan

Duplicates due to network lossage?

\*Hobbit\*

Info on RISKS (comp.risks)

### ✓ Outdated codes made US missiles useless

henry cox <cox@pike.ee.mcgill.ca> Tue, 21 Mar 89 10:25:50 EST

[ From the Montreal Gazette, 21 March 1989 ]

**OUTDATED CODES MADE U.S. MISSILES USELESS** 

WASHINGTON (Reuter) - The White House said yesterday obsolete electronic-launch codes were fed into an unspecified number of US land-based nuclear missiles several years ago, making them temporarily useless.

"In 1986, a few of the missiles in one squadron at Malstrom Air Force Base were

found to contain outdated codes. The actual number of missiles involved in the incident remains classified; however, the ... [sic] alert rate remained above 98 per cent," spokesman Marlin Fitzwater said. The base Fitzwater referred to is a Strategic Air Command installation in west-central Montana. He said the outdated codes, which would have kept air force personnel from launching the missiles in the event of war, were discovered during an annual code change. The presidential spokesman said launch codes for the 1000 US Minuteman strategic missiles are changed every year, as are codes at the country's 100 launch centres. "Presumably, the situation has been corrected," he said.

Fitzwater's comments were prompted by a report in the Washington Times, a right-wing newspaper with strong ties to the White House, which said it confirmed the error after an eight-month investigation. While Fitzwater said the exact number of missiles found to be inoperable is secret, he said: "There weren't very many of these missiles involved." The newspaper reported five of the 1000 US land-based missiles, each armed with three nuclear warheads, were temporatility disabled but it said the incident raises questions about the security and safeguards of all of them.

Henry Cox

[Also noted by <Walter\_Roberson@Carleton.CA> in today's Ottawa Citizen.]

# Risks of dying batteries

henry cox <cox@pike.ee.mcgill.ca> Tue, 21 Mar 89 10:06:56 EST

DYING BATTERIES CALL THE POLICE [ From the Montreal Gazette, 21 March 1989 ]

CLEVELAND (Reuter) -Dozens of calls to police and fire-emergency lines have been traced to cordless telephones that short-circui and dial 911 as their batteries start to die, officials said yesterday. One suburban police department said it received as many as 25 such calls a day. A Cleveland police communications expert said it appears failing batteries caused the devices to emit pulses that sometimes duplicated a 911 call.

[ Aside from the obvious nuisance factor, there is clear risk if emergency personel are accustomed to receiving many such calls - they may attribute the next inexplicable call to a faulty phone. Henry Cox ]

### Things to do with a computer...

Joe Morris (jcmorris@mitre.arpa) <jcmorris@mitre.mitre.org> Tue, 21 Mar 89 12:57:36 EST

The following item, reproduced in its entirity (without permission) from the 20 March issue of Digital Review (a DEC-oriented weekly) is both relevent to security discussions and funny to boot (pun intended).

COMPANY "SAW" SECURITY PROBLEM FOR MICROVAXES

You neven know what people are going to do next with a MicroVAX.

System managers at London's Midland Bank, one of Great Britain's largest clearinghouses, originally felt that their MicroVAXes should be located in the wholesale systems department.

But the folks who run MIS at Midland decided that this solution was not secure enough, and that the company's computer room would provide a safer location.

The security of the computer room, however, was called into question one weekend afternoon.

"On a Saturday, one of my guys went into the computer room and saw a carpenter in the process of modifying the room," said Jamie May, project manager for the wholesale systems department at Midland. This carpenter was using two of the MicroVAXes as a kind of workbench to try and balance the wood he was sawing.

"The dealers can sometimes be animals, but the computers would have been a lot better off and secure in the dealing room," May added.

### Possible Cancer Risks from Cellular Phones?

Mike Trout <miket@brspyr1.brs.com> 21 Mar 89 18:27:32 GMT

I recently had a discussion with a major electronics guru for a local television station. We were talking about microwave transmitters (radar speed guns, garage door openers, that sort of thing), when he made a dramatic statement that shocked me: he claimed that cellular phones were extremely hazardous and probably highly carcinogenic.

This is completely outside my area of expertise, so I can only repeat what he said. He claimed that the frequency wavelengths used for cellular phone radio transmissions were just about equal to the diameter of the human brain cavity. This, he claimed, accelerated by the fact that the receiver is always held up against the human skull, sets up highly dangerous conditions within the human brain. He said that ten years or so from now we're going to see an explosive increase in brain tumors among cellular phone users. He also claimed that some cellular units were far more hazardous than others, but that ALL of them are carcinogenic. He said he won't even work on them, and wouldn't wish a cellular phone on his worst enemy. This guy is rather eccentric at times, but his knowledge of electronics is legendary. His co-workers seemed to share his opinions; one of their technicians was severely injured some years back by climbing on a transmission tower during a high-intensity transmission. Whether this guy knows anything about human physiology is another question. Is this nonsense, an urban myth, or is this actually a matter of risk?

Michael Trout
BRS Information Technologies, 1200 Rt. 7, Latham, N.Y. 12110 (518) 783-1161

### Supreme Court and Copyrights

<ark@europa.UUCP> Tue, 21 Mar 89 14:44:59 EST

The US Supreme Court decided yesterday that state governments, including state universities, are immune to copyright laws.

I wonder what effect this will have on the software industry?

# Mitnick plea bargain

Rodney Hoffman < Hoffman. El Segundo @ Xerox.com > 20 Mar 89 18:43:17 PST (Monday)

An article by Kim Murphy in the 16 March 1989 'Los Angeles Times' reports on the disposition of the case against Kevin Mitnick, "who prosecutors said was as dangerous with a keyboard as a bank robber with a gun." [See RISKS 7.95 and 8.3 for earlier reports.] Edited excerpts from the latest article:

Mitnick pleaded guilty to one count of computer fraud and one count of possessing unauthorized long-distance telephone codes. He admitted penetrating a DEC computer in Mass., secretly obtaining a copy of a sophisticated computer security program which the company had spent \$1 million to develop. The program, said Mitnick's attorney, was designed to alert companies when their computers had been penetrated by hackers like Mitnick. Mitnick never attempted to sell or distribute the program, he said. Mitnick also admitted possessing 16 unauthorized MCI long-distance codes than enabled him to make long-distance telephone calls without charge. A prosecutor said Mitnick used the codes to make connections to computers.

Mitnick faces one year in prison. Under a plea agreement with the government, he must also submit to three years' supervision by probation officers after his release from prison. Prosecutors said they agreed to a 12-month sentence because the amount of financial damage was relatively low. DEC lost about \$100,000 to \$200,000 in computer "down time" investigating the security program theft. As part of the plea agreement, prosecutors agreed to dismiss two additional counts charging Mitnick with illegally accessing the Leeds Univ. computer in England and separate charge related to the DEC computer program.

### Re: Risks of telephone access to your bank account

Phil R. Karn <karn@thumper.bellcore.com> Mon, 20 Mar 89 13:50:29 EST

Brint Cooper makes the point that cellular phone isn't "telephone", it's radio. True enough, the braindamaged ECPA notwithstanding. But even calls placed

between conventional telephones can, on occasion, be almost as easily intercepted.

#### To demonstrate:

- 1. Obtain or set up a standard TVRO (Television Receive Only) satellite earth station. The receiver should have a "composite video" output jack (now pretty much standard, since VideoCipher descramblers need them).
- 2. Connect the aforementioned composite video jack into the RF input of a garden variety "shortwave" (HF) communications receiver set for single sideband (SSB) reception.
- 3. Aim the satellite dish at one of the AT&T Telstar satellites and find a transponder that doesn't seem to be carrying video.
- 4. Tune around below 6 MHz or so with the SSB receiver.

Rumor has it that dedicated circuits belonging to travel reservation services have been heard in this manner. Phil

### Internet Security Plans

Tue, 21 Mar 89 08:56:29 PST

INTERNET COMPUTER NETWORK TO USE CODE TO ENSURE PRIVACY By VIN McLELLAN, c.1989 N.Y. Times News Service

BOSTON -- Officials of Internet, the computer network that ties together hundreds of academic, government and corporate networks, are planning to begin a program that will permit users to send messages to one another in what is intended to be an unbreakable code. At present, users communicating over the network have little privacy. Sophisticated users can easily intercept and read messages. This lack of security has increasingly worried computer experts as the use of the networks has spread.

For many scientists and engineers, the networks have become a mainstay in their communications, used to exchange research results as well as carry on conversations that would otherwise occur over the telephone.

Under the new system, not only can an encrypted message be sent but the message will carry concealed information that will leave no doubt for the recipient that the person who says he sent the message did indeed send it. The recipient will also know with certainty that the message has not been altered.

Developers of the technology say the encryption will provide users with "digital envelopes" that cannot be opened except by the addressee, and the contents will have "digital signatures" that cannot be forged.

The encryption will be offered to 400 computer networks that are tied by the Internet network. The system will be based on one devised by RSA Data Security Inc. of Redwood City, Calif., that uses "public key encryption" techniques developed in the late 1970's by federally financed researchers at the Massachusetts Institute of Technology.

PKE, as the encryption technique is known, involves two "keys," one public

and one secret. Each user has a secret key and a public one that is published in a directory, just as phone numbers are. Someone uses the recipient's public key to send a message and the recipient uses his secret key to decode it.

The Internet proposal comes just as RSA and the Digital Equipment Corp. of Maynard, Mass., have agreed to give Digital full access to the same technology that Internet proposes to use.

DEC is expected to announce the agreement today. Digital officials said they expected to integrate RSA's technology into a broad array of software and hardware products. "The events of the past two years have shown that security has now become a necessary aspect of reliable distributed computing," said Robert Schleelein, manager of strategic relations for Digital's network and communications group. He was referring to numerous recent cases in which intruders have entered computer networks.

The agreement between Digital and RSA could give Digital a competitive edge in providing future computer equipment to users of the networks who want to take advantage of its new encryption technology. It will also probably mean that RSA's public key encryption technology, which is proprietary, could become the encryption standard on computer networks.

"Those of us who are involved in setting standards don't like to include in a standard anything that is a proprietary technology," noted Dr. Stephen Kent, chairman of the Internet Task Force on Privacy. "Adopting RSA, we have violated that rule of thumb, but we've done it with the full knowledge that we were doing it, and because we felt there were no other viable alternatives." Kent, chief scientist at BBN Communications Inc., in Cambridge, Mass., said the Internet standard was the result of more than two years of joint efforts by representatives from BBN, the Mitre Corp., the Xerox Corp., Digital, Texas Instruments Inc., University College in London, the Lawrence Livermore National Laboratory and the Commerce Department's Institute of Standards and Technology.

Digital's adoption and explicit endorsement of the RSA technology is itself a "tremendous advance in information security," said John O'Mara, executive director of the Computer Security Institute, an association of 3,000 corporate data security officers.

### Duplicates due to network lossage?

\*Hobbit\* <hobbit@pyrite.rutgers.edu> Tue, 21 Mar 1989 14:41:56 EST

Has anyone else been receiving complaints about lots of duplicate messages from people at particular sites? Some of these poor victims are getting on the order of 25 copies of one message. I've done some queue-watching and it appears that the SMTP dialog in these cases flies right along, no problem, until the . after the DATA, whereupon the remote host just sits there [ostensibly trying to deliver the message], and my end times out and requeues the message. Meanwhile the foreign end, not particularly caring that the sender nuked the connection, finally figures out what it was doing and delivers the message. While (stuck) repeat...

We've been having some network problems down here over the past couple of days, but one would think that once the connection is open and the dialog is running, you wouldn't get an inordinate delay \*ONLY\* after the DATA is sent. What's going on with these sites? Below I have included a list of offenders I could

find on the Security list. Any ideas? I'm running regular ole sendmail, and everything's working fine otherwise; it's just that these hosts refuse to acknowledge receipt of the message. They are running a bunch of different mailers, as well, so it isn't a problem with a particular type of mailer [although I've seen that sort of thing in the past].

Н\*

"slow" hosts follow:

AI.AI.MIT.EDU, asd.wpafb.af.mil, bbn.com, BCO-MULTICS.ARPA, cam.unisys.com, CCA.cca.com, CCINT1.RSRE.MOD.UK, cs.ucla.edu, EDN-VAX.ARPA, gateway.mitre.org, ibm.com, maths.bath.ac.uk, MITRE.ARPA, mitre-bedford.ARPA, mitre-gateway.arpa, mizar.usc.edu, msc.umn.edu, MWUNIX.MITRE.ORG, nems.arpa, opus.cray.com, prime1.lancashire-poly.ac.uk, RADC-TOPS20.ARPA, rand.org, relay.cs.net, relay.mod.uk, sdcrdcf.arpa, stony-brook.scrc.symbolics.com, stripe.SRI.com, tis.llnl.gov, ucbarpa.berkeley.edu, UCBVAX.BERKELEY.EDU, vaxa.isi.edu, vax.bbn.com, venera.isi.edu, wb3ffv.ampr.org

[I still get a monster BARFlist each time I send an issue. I try to be charitable before axing an address or a site. ("Clean up your axe?") 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 8: Issue 44

Tuesday 21 March 1989

# **Contents**

Computer-Justified Citations

**Kevin Driscoll** 

Vehicle ID tags, cont'd

Steve Smaha

Ethics question re fonts

**Michael Harrison** 

Elliott S Frank

Risks of shirt-pocket size floppy disks

**Roy Smith** 

Re: Pushbutton Banking

Robert English

Credit card magstripe-encoded pictures

Peter Scott

Re: Remote Smart-Cards, English and Welsh soccer

Craig Cockburn

**Dick King** 

Re: Risks of Registering Software

**Bill Murray** 

Collecting for Shareware

**Bill Murray** 

Info on RISKS (comp.risks)

# ✓ Computer-Justified Citations (Re: RISKS-8.40)

Kevin Driscoll <a href="mailto:driscoll@draco.src.honeywell.com">draco.src.honeywell.com</a> 19 Mar 89 19:45:21 GMT

Recently, in Atlanta, Georgia (GA), I was stopped and given three (!) traffic citations, when it was obvious that I was guilty of none:

"Offense":	Reality:
Turning where posted No L	eft Turn Not posted
Driving without valid licens	e Gave officer valid license

Driving without insurance Gave officer proof of insurance

I gave the officer my plastic Minnesota (MN) license, which indicated that it had just been renewed (MN clips the corner of the plastic card when a new one is ordered) and the temporary paper license that MN issues to cover the 45 day period it takes to make a new plastic card. The officer refused to accept this documentation! He said his computer did not show that I had a valid license. When I suggested that he retry his computer query (he may have made a mistake in typing, the GA or the MN computer or the connection between them could be having problems), he refused to do so!

His rationale for giving me a citation for no insurance was that I had signed the collision damage waiver for the National car I was renting. Apparently, he doesn't know that most major car rental companies are fully self-insuring for liability and he also doesn't know the difference between collision and liability insurance. He also refused the proof I had in hand that I also was covered by American Express, AND Honeywell, AND my personal MN liability insurance. I guess that none of this paper would stand up against his computer, which would only show GA insurance registration. Being quadruply insured with documents to prove it didn't help me at all.

The next day I saw an Atlanta newspaper article by Bette Harrison entitled "The Bureaucracy Zone" (in the style of the "Twilight Zone") about foul-ups in GA's handling of auto insurance information. The article tells how the GA Highway Patrol visited a man's house and confiscated his driver's license because of a clerical error. After explaining that GA insurance companies must inform the Department of Public Safety (DPS) of any policy changes, the article records the following conversation between the man's insurance agent and the DPS:

Agent: Look, if I send my policyholder down there with a letter from us indicating his policy didn't cancel, a copy of his insurance company's reinstatement notice, and a completed copy of your form O.C.G.A. 33-34-11 which we completed and and returned to you on Nov. 10, 1988 and he is stopped, what will happen?

DPS: He'll be arrested and his car will be impounded.

Agent: You've got to be kidding.

DPS: That is our procedure.

Agent: This is a clerical error and he is coming with the proof. Why should you penalize someone for a clerical error?

DPS: That is our procedure.

Agent to reporter: See, the machine that sits on their desk has become their God! They believe because the computer says it's right, it is. . . . . There are three issues here: the penalization of the American public due to our dependency on computers; the bureaucratic attitude that we experience at every level; and a system that doesn't have safeguards to prevent the innocent from being victimized along with the real violators.

I can confirm what the agent said. GA gave me two options, plead guilty or go to court. Pleading guilty to three moving violations (yes, in GA license and insurance are also moving violations) would mean loss of my license when GA forward the guilty info to MN. MN suspends licenses for 3 moving violations in 6 months. This happened on a Thursday. The officer said he only appeared in court on Mondays. But next Monday was too soon. It seems that GA's computer system can instantly accuse me of crimes, but it takes more than four days to get information from the police department to the courts!

Just before I left GA on the following Wednesday (almost a week later), I went to the Traffic Court to see if I could straighten things out. The citation information hadn't gotten there yet! I told the clerk my story, and said that I had, with me, the proof of license and insurance. She said, "OK, give me your copy of the citation and the fine and we can process it." Fine? She thought I was pleading guilty. Bringing in proof of license and insurance (if you have them) is required to plead GUILTY! Not only must a driver have both, but also must have them in the car when driving. Bringing them in later is no proof of not being guilty.

I spent all of that afternoon convincing the Court to let me see a judge and to plead not guilty. The majority of the cases I witnessed while waiting for the judge were license and insurance citations. In the first concession to reasonableness I had seen in this affair, I got the license and insurance citations dropped. However, the judge said I would have to come back for the No Left Turn citation. I had to be in California the next Monday, so I asked if I could do it by deposition through the mail. No, I had to appear in person. So one can be accused by remote information by cannot use the same process for defense. Not being able to be in Atlanta, I have pleaded nolo contendere under duress. I nolo plea HAS to be handled through the mail and can be accepted or rejected by a judge. I am still waiting for the outcome.

The moral: When in GA, watch out, that caricature of southern justice may now have silicon help.

P.S. You would think that Atlanta, which is trying to be a major convention city, would have special provisions to make things easier for out of state visitors. Because just the opposite appears to be true, I will stay clear of Atlanta. Also the conventions and meetings that I have influence over will also not be in Atlanta.

Kevin R. Driscoll, Principal Research Scientist (612) 782-7263 FAX: -7438 Honeywell M/S MN65-2500; 3660 Technology Drive; Mpls, MN 55418-1006

[In the old days -- 40s, 50s, maybe even 60s -- Georgia was famous for its speed traps, e.g., 15 mph (poorly marked) for a few yards in the middle of a stretch of 45 mph, with squad cars and a judge sitting there waiting for unsuspecting out-of-staters. Apparently "Poli want a Cracker" is NOT the operative principle -- except maybe for Floridians. PGN]

### ✓ vehicle ID tags, cont'd

Steve Smaha <Smaha@DOCKMASTER.ARPA>

Tue, 14 Mar 89 21:33 EST

From the 6 March 1989 PC Week:

Like every other U.S. airport, San Francisco International always charged a monthly fee to the rental-car and hotel courtesy vans that sweep through its terminal areas to pick up customers.

But the flat rate became problematic. Courtesy vehicles, free to swarm through ground-transportation areas as often as they liked, jammed up the limited space in passenger pick-up areas. Airport managers even began suspecting courtesy vans were driving into passesnger areas "more for advertising than for carrying people," said Sheldon Fein, airport manager of traffic control.

Now, the airport is pioneering a PC-based system it hopes will relieve traffic congestion and help it bill courtesy providers for every time they cruise by.

The airport is requiring vehicle [sic] to mount radio-frequency identification tags on the roof of each vehicle. Each electronic tag, made by General Railway Signal Corp. of Rochester, N.Y., emits a unique ID code that's logged automatically by overhead receiving boxes every time a vehicle drives into a ground-transportation area.

The receivers link by modem to a back-office PC AT, where custom-developed software help bill vehicle operators accurately and report on driver activity. Now, instead of \$50 to \$100 a month, vehicle operators pay 35 cents a trip. The fee will hit \$1 next January. Fein believes this will reduce traffic jams and create an airport profit center.

[There are other vendors for such systems, as well. I wonder what the reset time is for a sensor? If I drove my (slightly-modified) personal vehicle slowly beneath a sensor, could I enrich the Airport with hundreds of my competitors' dollars? Could I trigger every sensor in the area? Would they receive an appropriately itemized bill? Would anyone (except Cliff Stoll) even notice?]

#### Ethics question re fonts

Michael Harrison <harrison@mahogany.Berkeley.EDU> Tue, 21 Mar 89 09:07:47 PST

Several colleagues have been kind enough to tell me about the message sent to the Risks Forum by Randall Neff of Stanford University concerning my recent seminar talk on the VorTeX project.

In this note, I hope to set the record straight and to clear up Mr Neff's misunderstandings.

- 1. As Mr. Neff indicated, the VorTeX group implemented an interpreter to display PostScript on our workstations. Adobe has given us a license to use their PostScript commands in this software.
- 2. It is also the case that in order to preview output, we needed outline fonts. When we inquired about the use of Adobe fonts, we were told that they

were not available (at any price). I attempted to obtain fonts from Bitstream, but their price of \$85,000 plus royalties was beyond our means for research software.

Mr. Neff's quotations are erroneous. I never objected to Adobe's refusal to let us use their fonts. That is their right. I did express concern that commercial interests were forming an impediment to research in document processing.

- 3. In the US, type faces may not be copyrighted (although their names may be trademarked). It has always been perfectly legal to measure or photograph characters appearing in a book, for example, and to use those measurements or images for the type face of some other manuscript. In our case, we wrote Postscript code that measured the characters of various fonts, and then used curve fitting to reconstruct approximations to the shapes of the original characters. As I indicated in my talk and others have discussed in this forum our methods were legal and proper. It is unfortunate that Mr Neff thought we were trying to put one over on Adobe. He alleges that we acquired Adobe's product. This is certainly incorrect. In particular, we did not try to extract the "hints" that make low-resolution rendering possible, although others done so.
- 4. Once we had devised this approach, which seemed to solve our problem, I phoned a senior staff member at Adobe to report what we had done and to find out if Adobe had any problems with it. After telling me that he knew a faster way to do what we were doing (but not indicating what it is!), he said that he would report it to management and that I should expect a call. A day later, I received a call from the Adobe general counsel requesting only that I obtain a license for the use of the PostScript instruction set. We honored that request.

Thus not only do I see nothing unethical about our behavior, Adobe has registered no objection.

5. Finally, let me mention that there was a formal question/answer session at the end of my seminar. I stayed around afterwards talking with people. After that, there was a dinner to which all interested parties were invited. Mr Neff had ample time to raise ethical or any other issues with me had he chosen to do so.

[Messages from Mike Haertel and Kenton A. Hoover reiterated one or two of Mike's points, and are omitted here. PGN]

## ★ Re: reverse engineering of type fonts

Elliott S Frank <esf00@uts.amdahl.com> Fri, 17 Mar 89 10:09 PST

This latest controversy [about UCB "reverse engineering" Adobe fonts] smells suspiciously like the incident several years ago in which another UC campus duplicated and distributed around the campus multiple copies of a CAD package. When sued by the owners of the CAD package, the successful defense was that the Regents of the University of California \*are\* the State of California, as so

far as the law is concerned; and, under the Constitution, a State may only be sued with its consent and the Regents did not consent to be sued.

This suggests that under current case law, there is a significant commercial risk in selling (or, far worse, allowing to be sold) intellectual property, or anything containing significant intellectual property, to, at least, anyone involved with the UC system. Since it appears UC is not bound by the usual "fair use" rules of copyright, we may now start to see strange restrictions in the "shrink wrap" agreements as companies and their lawyers attempt to protect their products.

Elliott Frank ...!{hplabs,ames,sun}!amdahl!esf00 (408) 746-6384 or ....!{bnrmtv,drivax,hoptoad}!amdahl!esf00

[the above opinions are strictly mine, if anyone's.]

## Risks of shirt-pocket size floppy disks

Roy Smith <roy@phri.phri.nyu.edu> Tue, 21 Mar 89 11:31:57 EST

I suddenly remembered just now that 1) I don't remember taking the 3.5" floppy out of my shirt pocket last night and 2) My wife was doing laundry this morning. Yet another risk to data integrity. Gives another definition to "cleaning out your old files". We didn't have these problems back in the old days; when's the last time you forgot to take a reel of tape (or a deck or cards!) out of your pocket before doing the laundry?

#### Re: Pushbutton Banking (Lynn Grant, RISKS-8.38)

Robert English <renglish%hpda@hp-sde.sde.hp.com> Mon, 20 Mar 89 11:14:01 pst

I found this message highly disturbing. Not only did this obvious weakness not occur to the bank, but after it had been pointed out, there solution was removing the individual that noticed from the system, rather than doing anything to fix the problem.

--bob--

## Credit card magstripe-encoded pictures

Peter Scott <PJS@grouch.JPL.NASA.GOV> Sat, 18 Mar 89 11:17:19 PST

[A comment on Henry Spencer's comment in <u>RISKS-8.40</u> on Ruaridh Macdonald's "A Touching Faith in Technology", <u>RISKS-8.35</u>]

An item that could be encoded on the magstripes in credit cards that would pose little privacy risk while enhancing protection for the consumer would be a

digital image of the credit card holder. When they apply for their card they send in a picture, and their card's stripe is encoded with a compressed image, say 100 \* 100 \* 8 bits. A display terminal would be small and reasonably cheap in mass production, and would end a great deal of credit-card fraud. I see no disadvantage to the consumer. Of course, if they just laminated the photograph on the credit card in the first place... but perhaps using the stripe would be easier since it requires no time-consuming human intervention in the card fabrication process, and the company could store your digitized image along with your account information. (Which provides new possibilities for verifying your identity over the telephone: "So, sir, do you still have that wart on the left side of your nose?" "What wart?" "That's what I wanted to hear. How may I help you?")

Peter Scott (pjs@grouch.jpl.nasa.gov)

## ★ Re: Remote Smart-Cards (for English and Welsh soccer) (RISKS-8.41)

Craig, PhaseV & FCNS <cockburn%marvin.DEC@src.dec.com>
21 Mar 89 11:08

The bill I believe only requires ENGLISH and WELSH football clubs to enforce the card ID scheme. Scotland is EXEMPT from this scheme, probably for much the same reasons as ENGLISH and WELSH teams were banned from playing on the continent (and still are), whereas Scottish teams ARE NOT.

Please use the term 'English and Welsh' instead of UK, when the bill does not apply to Scotland (I don't know the exact situation in NI). Scotland has it's own laws, and is proud to remain separate from its southern companions.

Craig. cockburn@marvin.wessex.co.uk

[Hmm. Amusing that this message follows contributions from English and Scott? But no one is Welshing. PGN]

#### Remote Smart-Cards (RISKS-8.41)

Dick King <king@kestrel.arpa> Tue, 21 Mar 89 09:01:28 PDT

Why is writability necessary for anti-passback? Seems to me that remembering what cards have been used is more than sufficient.

Putting writable cards in the hands of the public and trusting what they say would be just "asking for trouble" in this country, and likely so in other countries. The one thing you probably want to be able to say to a card is "please, card #1234, don't squawk for ten seconds", so the electronic turnstile could make sense out of a crowd. But even this is probably unnecessary with careful design.

#### ★ Re: Risks of Registering Shareware

<WHMurray@DOCKMASTER.DCA.MIL>
Tue, 21 Mar 89 08:13 EST

There seems to be an implicit assumption here, and in other discussions on RISKS, that simple possession on my credit card number is all of the authorization that one needs to charge me. It should be noted that all of the ethical people with whom I do business by credit card do have my number. They do not re-use it for the simple reasons that they are ethical AND that I can disown the transaction. You see, not only must you have my number, you must also have my consent. While it is true that possession of the number transfers the burden of action to me, the burden is still on you to prove that you have my consent. In the absence of some other evidence on your part (such as a receipt for the delivery of goods), a simple assertion on my part that you do not have my consent is sufficient.

Note that in the credit card system, my right to disown the transaction persists even after you have received your money. This is a much better remedy than is available to me if you have gotten your money by currency or check.

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

## ✓ Collecting for Software

<WHMurray@DOCKMASTER.DCA.MIL> Tue, 21 Mar 89 08:32 EST

Many of the control problems that are suggested here will be dealt with through the application of digital envelopes (to prevent the disclosure of the credit card number) and digital envelopes (to demonstrate your intent to pay for the software and to enable you to disown any transactions not so signed.)

However, two other innovative methods for distributing and collecting for software are being used by companies engaged in selling crypto products. For example, EnigmaLogic, who sells one-time password software, has a license fee that is based upon the number of users that you employ it for. If you want to change the number, you call them. They give you a one-time password that can be used to adjust the software and they adjust your bill accordingly.

RSA Security Inc. market public/private key software. They will freely distribute the software, but charge you a license fee for it only when you wish to register your key.

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 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 8: Issue 45

# Saturday 25 March 1989

## Contents

Wells Fargo Deposits Slip

**PGN** 

Hospital Viruses

**Dennis Steinauer and Joe Morris** 

Optical Scanning of Handwritten Purchase Orders

**Hiram Clawson** 

Credit card magstripe-encoded pictures

Mike Trout

Cellular phones and health

anonymous

Dale Worley

R. Scott Truesdell

New method (risk) of demagnetizing floppies Douglas B. Robinson

Microwave ovens

**Don Chiasson** 

Corrections to Internet Security Plans

David M. Balenson

Info on RISKS (comp.risks)

#### ✓ Wells Fargo Deposits Slip

Peter Neumann < neumann@csl.sri.com> Sat, 25 Mar 1989 14:16:46 PST

A computer software glitch at Wells Fargo Bank has caused a delay in depositing payroll funds for 12,000 to 15,000 workers at about 70 companies, mostly in Northern California. (The delay of a day or weekend apparently affects only people whose paychecks are deposited automatically on a weekly basis. This was considered a drop in the bucket, because WFB processes about 1.5 million payroll accounts each month. SFB promised to cover any overdraft charges.) [Source: San Francisco Chronicle, 25 March 1989, p. B4]

## Hospital Viruses -- Now things are REALLY getting confusing.

"STEINAUER, DENNIS" <steinauer@ecf.icst.nbs.gov>
23 Mar 89 21:13:00 EDT

The following was in the 3/23/89 Washington Post (and probably other places, since it came over the newswire. Lots of comfusing and seeminly contradictory info. Anyone know anything about it? dds

COMPUTER VIRUS STRIKES MICHIGAN HOSPITAL Records Altered or Scrambled but Patients Were Not Endangered

BOSTON, March 22 - Computer viruses, which have disrupted university, newspaper and government systems, have spread to hospital computers.

Officials at William Beaumont Hospital in Royal Oak, Mich., said two viruses altered or scrambled patient information in a computer that creates high-quality pictures for diagnosing diseases.

The viruses, according to a report in the New England Journal of Medicine Thursday, also created non-existent patients and spread to two other medical facilities.

Dr. Jack E. Juni and Richard Ponto of the Beaumont Hospital said patients were not endangered by the virus because original copies of the records were not stored in the infected computer.

A computer virus is a malevolent computer program designed to spread itself surreptitiously throughout a computer system and, before anyone realizes it is present, destroy or alter stored information.

The new case is being reported as doctors and hospitals are developing growing reliance on all-purpose computers far more vulnerable to infection by viruses.

Ponto and Juni said the Beaumont virus was discovered when the hospital's new image-display station, which creates pictures for heart studies, stopped responding to commands. Then nonexistent patients and garbled names appeared on the patient directory.

When officials investigated, they discovered that seven of 10 programs had been altered and that the virus had created many new files.

Juni said the virus was on a hard disk manufactured by CMS Enhancements of Tustin, Calif.

CMS spokesman Ted James said a virus, inadvertently put on 600 such disks last October, had contaminated a program used to format the disks. The virus apparently entered the company's plant on a hard disk returned for servicing.

James said the virus was "as harmless as it's possible to be." It inserted a small piece of extra computer code on hard disks but did not reproduce or tamper with other material on the disk.

[Also noted by Joe Morris]

#### ✓ Optical Scanning of Handwritten Purchase Orders

<hiramc@sco.UUCP>
Fri Mar 24 17:00:51 1989

Seen on the order form for Microsoft QuickC Ver. 2.0 Update:

"To quickly and accurately process the large volume of orders that we receive, we have installed an optical scanner that will read and code your coupon. To ensure the fastest possible fulfillment of your order, when filling out the coupon, print your characters so that they look exactly like those in the sample below (take special notice of the "o")."

That last line was in italics, and there followed the alphabet and numbers as we are supposed to print them. The "o" looked like a Q rotated 180 degrees.

I thought the computers were supposed to adapt to us rather than the other way around?

--Hiram Clawson - uunet!sco!hiramc | hiramc@sco.COM 408-458-1422 ext. 3289

## ✓ Credit card magstripe-encoded pictures (RISKS-8.44)

Mike Trout <miket@brspyr1.brs.com> 23 Mar 89 20:01:55 GMT

> ... I see no disadvantage to the consumer.

I do. Once this starts up, it will be only a matter of time before they start taking digitized images of you ("cheap line-scanning monochrome cameras!") each time you attempt to use the card. The bits of this "current" image will then be electronically compared to the bits of the "original" image. If the match-up is less than, say, 99%, or maybe 95%, or maybe even 90%, it's "sorry, charge not approved..." Who decides the percentage of match-up allowed?

Even assuming the digitized image is only "one-way," that is, only appears on a screen for a clerk to compare to your face as you stand there with hat in hand, there are serious potential problems. In either case, consider the following scenarios: Two or three times a year, I drastically change my facial hair (clean shaven, mustache only, mustache plus beard, etc.). And what of folks who have plastic surgery, either by choice or because of disfiguring accident? And those who have accidents and can't afford surgery? Men going bald? Women (and men!) who drastically change their hair styles? Differences in makeup application? The basic aging process? Are we all to be locked into one appearance?

And what of the complexities of the individual human face? By slightly flexing a few facial muscles, anyone can transform their face into something new. Meryl Streep is an extreme example. What of the guy who has his original photo taken the day after he is married, and then applies for some credit the day after his wife informs him she is filing for divorce? You know that any digital representation of his face will have considerable bit differences.

Will this image exclude any clothing that appears below the neck (collars, ties, etc)? If not, you'd better be sure to wear exactly the same thing every time you use your credit card ("uh, wait, lemme try tying my tie a little differently..."). And what of differences in light and shadows?

Many will argue, "but those same problems COULD exist with any photo ID, but there are no such problems in real life." Absolutely true. But once something has been "computerized" it takes on God-granted status. In the last issue of RISKS, Kevin Driscoll treated us to the bizarre story of how the Georgia Department of Public Safety is completely unwilling to correct errors entered into their computers, even when they know about those errors. Try explaining to an 18-year-old clerk that she shouldn't worry about the fact that you "look different" from your computerized image ("I'm sorry, sir, but that's what's in the COMPUTER..."). People can adjust for changes in a photograph, such as those on most driver's licenses. But that image on the "computer screen" may as well be carved in granite.

#### > ... "What wart?" ...

I find such personal inquires repugnant, and would have a hard time avoiding slamming down the phone. But on a more important topic, is there any empirical evidence to suggest that credit card fraud could be significantly reduced by facial images, either true photographs or digitized images? I am reminded of the controversy in New York State a few years back, when we became the last of 50 states to place a photo ID on driver's licenses. Some enterprising reporters actually went so far as to talk to law enforcement officials about the value of photo IDs. The consensus, even among the sometimes over-enthusiastic State Troopers, was that there was no real law enforcement use for photo IDs. Alternative methods of investigation are far more useful. NSA food: Iran sells Nicaraguan drugs to White House through CIA, SOD & NRO.

Michael Trout, BRS Information Technologies, 1200 Rt. 7, Latham, N.Y. 12110 (518) 783-1161

#### cellular phones and health

<[anonymous]> Wed, 22 Mar 89 10:11:18 PST

It is fairly well established that exposure to high relative power densities of UHF and higher RF frequencies can cause significant health problems. Parts of the body that are the most sensitive to heat effects are the most vulnerable to RF effects, with the eyes being the most sensitive of all. There have been cases of police departments having problems with officers who developed cataracts apparently relating to their use of hand-held UHF (e.g. 450 Mhz) transceivers.

Hand-held cellular phones are probably even worse. Like police transceivers, these units almost always have the antenna in very close proximity to the user's head, putting the head (and eyes of course) in a quite strong relative field (while the absolute power may only be a few watts, the relative power density near the antenna is quite high). Also, cellular units operate at around twice the frequency of police transceivers (i.e., cellular operates around 800 Mhz and higher) and the higher the frequency, the worse the risk.

Another factor is that while police transceivers are half duplex and only transmitting when the officer has something to say, cellular transceivers are transmitting continuously when a conversation is occurring (since they are full duplex) so the overall exposure is far higher in most situations.

It would appear that a real risk may exist.

Note that the farther you get away from the antenna, the better off you are, since the inverse square law applies.

### Risks from cellular phones

Dale Worley <worley@compass.com> Fri, 24 Mar 89 10:53:08 EST

From: miket@brspyr1.brs.com (Mike Trout)

Subject: Possible Cancer Risks from Cellular Phones?

I recently had a discussion with a major electronics guru for a local television station. We were talking about microwave transmitters (radar speed guns, garage door openers, that sort of thing), when he made a dramatic statement that shocked me: he claimed that cellular phones were extremely hazardous and probably highly carcinogenic.

Sorry, but this is extremely unlikely. Human flesh is very poor at absorbing (or affecting in any way) radio waves. Because of this, possible resonance effects between the skull and the transmissions are very unlikely.

There are three ways that electro-magnetic radiation can harm living tissue: (1) electric-current burns. This is what gets people who touch or come very close to high-power antennas. (To be precise, however, this effect is due to inductive or capacitive coupling with the antenna, rather than absorption of E-M radiation.) (2) thermal heating due to resonance absorption (usually by water molecules). This is how microwave ovens heat things. However, this effect can happen only at certain specific frequencies of radiation, all of which are much higher frequencies than are normally used for cellular phones. [These first two effects cause problems only at high power levels, because the human body can take a significant amount of current flow and heating without any damage at all -- at low power levels, they are lost in the noise of biological currents and heat generation.] (3) direct modification of molecules. This happens only with high-energy E-M radiation, X-rays and gamma rays. [This is the only one of the three damage mechanisms that can cause cancer.]

As you can see, it is unlikely that a cellular phone will harm you via any of the three mechanisms, much less cause you cancer.

I'm not particularly astonished that this fellow is worried that pressing a radio transmitter to your head might be harmful, although he should have done a bit of research before spreading groundless warnings. I am astonished that he thinks they cause cancer. I can see no reason for even

an uninformed person thinking this, other than the "Everything bad causes cancer" scare-mentality that seems to be popular.

I once read an article noting that over the last 10 years there were several dozen alleged risks to human health that had achieved enough newspaper coverage to seriously scare people, and it noted that while a few of them were indeed serious health risks, most of them were, in practice, harmless. It also noted that the information presented in newspapers was almost useless for distinguishing these two categories. I wonder what will happen when "cellular phones cause brain tumors" hits the papers?

The RISKS of needless and wasteful regulation of non-threats (not to mention of hardening people to the point that they fail to be concerned about genuine health risks) are, as people say here, obvious. When will some sanity be injected into the subject?

Dale Worley, Compass, Inc.

worley@compass.com

#### Cancer from Cellular Phones

<truesdel@PARIS.ICS.UCI.EDU>
Wed, 22 Mar 89 10:01:52 -0800

Cellular phones operate in the 800 MegaHertz band. This is in the middle of the UHF band, directly below the microwave band. Microwaves, as we all know, are used for making popcorn and cooking turkeys.

800 MHz puts the full wave right at 14.8 inches or a half wave at 7.4 inches which is a little long to resonate inside the skull cavity. This doesn't mean that it can't cause real damage, though. An example has been showing up since civic police forces have started switching up from the VHF to the UHF bands for local communications. The advantages of using higher frequencies are more bandwidth, less interferrence, and better audio quality. The RISKS, however, are starting to show up.

The problems were first noticed in officers making extensive use of hand held (walkie-talkie) units with built-in "Stubby-Duck" antennas. These antennea are identified by have a length of around 2 - 4 inches, a diameter of about a quarter inch, and made usually with a black rubber coating. When held in the talking position, the antenna is positioned in close proximity to one of the eyeballs. That's when the glaucoma started showing up. Essentially, the UFH waves were frying the aqueous humor... turning what should have been the consistency or Jello brand gellatin desert into the consistency of 3 day old oatmeal.

So the local P.D.s decided to move the radios away from the face and strap them onto the officer's belt. The interaction is through a hand-held speaker/mic. Great solution! Now the officers get it in the spleen instead of the face!

So, back to cellular phones. Hand-held units with built-in antennas are obviously the greatest risk. Antennas placed on the roof of the car, shielded by the cars sheet metal, are best. This assumes that the installation was

competently made by a knowledgeable RF technician (NOT a stereo installation jocky), the connectors are "low loss", and the coax itslf is "low loss". The most common cellular phone coax is cheap RG-58/U. This is "thin ethernet" cable. A much safer connection is made the thicker coax (I think RG 59/U, but I don't remember). The thin stuff is used more because it is cheaper and MUCH EASIER to install.

I am very interested to see what further studies are being conducted relative to the long term effects of exposure to RF. I am worried about the unrestricted saturation we receive 24 hours a day on all frequencies. How free of effect are the "safe" frequencies (VHF, HF)?

R. Scott Truesdell

[Please pardon a little redundancy. I could not prune easily. PGN]

## New method (risk) of demagnetizing floppies

<robinson@apollo.com> Fri, 24 Mar 89 13:11:46 EST

One fine \*cold\* day in February I transported a floppy from location A to location B. I thought nothing about placing the floppy in the passenger chair. It was positioned vertically against the chair back, wedged gently behind an empty child seat. The trip took about 30 minutes. Then I tried to read the floppy and could not: the machine couldn't even find track 0. I tried about a half-dozen or so machines before I gave up.

It was an old floppy so I guessed that it just couldn't hold the bits anymore, so I got a few new ones and was going to try again when the real cause of the problem dawned on me: I own a 1985 SAAB with the \*heated\* front seats. I guessed that since the heating element was electrical it might be puting out enough of a magnetic field to scramble the data. So I experimented: I made about 5 copies of the floppy and placed some of them on the floor and one of them on the seat as before, drove for about 30 minutes (again on a cold day) and then tried to read them. The floppy placed like the first one was unreadable. Those on the floor were fine.

I'd sure like to get a instrument and measure the magnetic field near that chair when the heater is working. I'd like to know why the magnetic stripe on the credit cards in my wallet still work...

Douglas B. Robinson

#### Microwave ovens

Don Chiasson <G.CHIASSON@XX.DREA.DND.CA> Wed, 22 Mar 89 16:13:34 AST

A few nights ago a minor incident occurred which typifies how computer risks can be worse than those of other technologies and why people get

upset. At about 2:00am, my toddler woke up demanding nourishment so I put 250ml of milk in the microwave to heat. It was dark and I wasn't too well coordinated with the result that I spilled the milk. Most went on the kitchen counter, some on the touch pad and a few drops went into the door latch mechanism. I cleaned the mess, heated more milk and all was fine.

The next morning was not quite so fine: the microwave worked normally except that it turned on when the door was open! A small amount of milk had seeped (I suspect through the door latch) into the electronics causing a bizarre and highly unsafe failure. I was especially disturbed because a microwave hazard is invisible.

My point is that a very important safety requirement - the magnetron must not be on when the door is open - had been implemented in logic with other routine functions. An old design would have used a mechanical switch to disable the magnetron when the door was open. Computerized logic systems allow inexpensive implementation of a broad range of features by treating all functions and all signals uniformly. Unfortunately, such uniformity does not normally permit special safeguards for critical functions. A robust design would use separate systems for activation and safety.

# Corrections to Internet Security Plans (RISKS-8.43)

David M. Balenson <br/>
<br/>
Thu, 23 Mar 89 15:00:06 EST

For the record ...

... the New York Times article by Vin McLellan on March 21st (Volume 8, Issue 43) regarding the "Internet Security Plans" incorrectly included Texas Instruments (TI) Inc. in the list of representatives responsible for the Internet standard. In fact, Trusted Information Systems (TIS) Inc. a small privately-owned computer and communications security consulting firm based in Glenwood, Maryland is one of the representatives responsible for the Internet standard. Furthurmore, Dartmouth College was inadvertently ommitted from the list of representatives.

I should also mention that the article fails to point out that the Internet mail messages themselves are actually protected using the Data Encryption Standard (DES) and that RSA is only used to protect and distribute the DES keys.

-David M. Balenson, Trusted Information Systems, Inc. (301) 854-6889



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 8: Issue 46

# Wednesday 29 March 1989

## **Contents**

B-1B wept-swing swept-wing

**PGN** 

Soviets Lose 2nd Mars Probe

**PGN** 

Satellite failure due to unremoved lens Cap

Technology strikes again -- Dodge Spirits and Dodge Fever

Matt Fichtenbaum

Suing over runaway computer systems

**Rodney Hoffman** 

Virus Hits Hospital Computers

**Rodney Hoffman** 

Prank Virus Warning Message

Bruce N. Baker

Subversive bulletin boards

**Eric Percival** 

UK Computer Threat Research Association

David J. Ferbrache

Will the Hubble Space Telescope Compute?

Paul Eggert

The Airbus disaster and Ada

Ted Holden via Bob Burch via ipff

DIAC-90 -- Call for Papers

**Douglas Schuler** 

Info on RISKS (comp.risks)

#### B-1B wept-swing swept-wing

Peter Neumann < neumann@csl.sri.com> Wed, 29 Mar 1989 10:49:24 PST

The Air Force temporarily grounded its fleet of B-1B bombers yesterday after the wings on one of the planes malfunctioned just before a training flight... The crew could not get the plane's wings to move back and forth

in tandem and, at one point, the left wing apparently moved too far forward and punctured a fuel tank inside the fuselage. The wings are normally swept back for high-speed attack runs and forward for takeoffs and landings...

The B-1B still has problems with its radar-jamming gear... [San Francisco Chronicle, 29 March 1989, p. A11]

#### Soviets Lose 2nd Mars Probe

Peter Neumann <neumann@csl.sri.com> Wed, 29 Mar 1989 10:51:29 PST

The Soviet Union has lost radio contact with its backup spacecraft to Mars and the Martian moon Phobos... In September 1988 the Soviets lost contact with the first of the twin Martian probes, Phobos I. [See <u>RISKS-7.53</u> and 56.]

### Satellite failure due to unremoved lens cap

Peter Neumann <neumann@csl.sri.com> Wed, 29 Mar 1989 10:56:52 PST

A \$140 million Star Wars Satellite [launched on 24 March] failed one of its first tests... The satellite was meant to observe the firing of a nearby rocket in space but was unable to do so because a lens cap blocked its view. The lens cover stayed on a sensor too long, blocking it from tracking the second-stage engine as it drifted away in space. As a result, the satellite was pointed in the wrong direction to view the longer of the second-stage firings. [San Francisco Chronicle, 28 March 1989, p. A10]

#### ✓ Technology strikes again -- Dodge Spirits and Dodge Fever

Matt Fichtenbaum <mlf@genrad.com> Mon, 27 Mar 89 16:22:43 EST

I test-drove a Dodge Spirit last week. It had Chrysler's new 4-speed overdrive automatic transmission, which is controlled electronically.

As we were sitting in the car before beginning the test drive, the salesman folded down his sun visor, noted the vanity mirror built into it, and said, "Illuminated mirrors! How nice!" So I folded down \_my\_ visor, lifted the cover on the mirror, and noticed that the lights didn't light. "How did you make yours light?" I asked. "They won't, until we connect a connector under the hood," said he, "we disconnect things that might drain the battery if left on inadvertently." I resolved to check the mirror illumination later.

So I drove out from the dealer's lot, accelerated gently to about ten miles per hour, and notice that the transmission had not yet shifted up. "Shift, you!" said I. The salesman then started to laugh embarrassedly and remembered that the transmission controller needed "that connector" reconnected.

This time the Spirit wasn't quite willing.

[And the Flashers were weak... PGN]

#### Suing over runaway computer systems

Rodney Hoffman <Hoffman.ElSegundo@Xerox.com> 29 Mar 89 10:41:46 PST (Wednesday)

Edited excerpts from a feature article by Jeffrey Rothfeder in 'Business Week' magazine April 3, 1989:

USING THE LAW TO REIN IN COMPUTER RUNAWAYS

MORE UNHAPPY BUYERS ARE TAKING SYSTEMS SUPPLIERS TO COURT

Geophysical Systems Corp. hired a Raytheon Corp. subsidiary, Seismograph Service Corp., to build a \$20 million computer system to process sonar-generated data. The system couldn't do it. Geophysical's clients canceled their contracts, and Geophysical entered bankruptcy. Last December, a Los Angeles jury awarded Geophysical Systems Corp. \$48.3 million from to cover computer-system costs and lost profits, although the judge has ordered a new trial to review the size of those damages.

Geophysical had claimed that the Seismograph system couldn't meet its complex computation requirements -- and that Seismograph knew this before it started building the system. By finding for his client, says Geophysical's attorney, "the court is saying that if we wanted a computer unable to handle our data we could have gone to Toys 'R' Us and been out \$20 instead of \$20 million."

As computer runaways -- systems that are over budget, installed late, or don't work -- become endemic, fed-up customers are fighting back. And they're using the law to do it. In 1988 the American Arbitration Assn. took on 190 computer disputes, most of them concerning defective systems, totaling \$198 million in claims. That was up from 123 cases in 1984, representing claims of \$31 million. Dozens of law firms now specialize in high-tech matters.

[More tales of (smaller) cases.] When a customer sues, it loses its computer supplier. It may take years to find a replacement and build a new system -- not to mention win the original suit. Because of this, says one attorney, "when you sign a contract for a computer system, you're locked in a deadly embrace with the supplier that you not be able to, or want to, get out of." The boilerplate agreement that suppliers typically offer includes numerous so-called exclusions of warranty that limit the supplier's liability for system failures or delays. Also, the contract usually states that nothing in it is binding unless specifically spelled out.

A former Price Waterhouse senior consultant recalls telling customers that it will take "only 72 hours for a crucial software project. But we wouldn't put this into the contract. Then when it took us two months to do the job, we simply explained that the project now costs more because the extra work we did was out of the scope of our agreement."

The State of New Jersey reached a settlement with Price Waterhouse over a bungled system to handle licensing and traffic violations for the Motor Vehicles Dept. During nearly two years of negotiations, the accounting firm fixed the system. New Jersey got the system for \$1.2 million less than the contracted price, and Price Waterhouse swallowed approximately \$2 million in additional project costs.

Many customers are starting to demand contract clauses providing for binding arbitration of disputes, and for acceptance tests before the customer pays.

Surprisingly, the new legal aggressiveness of customers isn't particularly troubling to most systems suppliers. Customer activism may even reduce the number of runaways from an estimated 35% of all current computer projects. Says a systems designer at one Big Eight accounting firm: "It could be just the thing we need to make us more honest."

A sidebar lists THINGS TO DEMAND WHEN BUYING A COMPUTER SYSTEM:

- \* ACCEPTANCE TEST. Requires the supplier to run the customer's actual data successfully through the system.
- \* GUARANTEE. The customer pays leasing or purchase charges only after the new system has been working correctly for two months.
- \* BINDING ARBITRATION. Stipulates that the customer can elect to have disputes resolved by an outside arbitrator.
- \* SOFTWARE OWNERSHIP. Give the customer the rights to the system's source code and leaves it in the customer's possession.
- \* SUPPORT. Guarantees that support and servicing for the system will be available for at least a year -- even if the supplier goes out of business.

### ✓ Virus Hits Hospital Computers

Rodney Hoffman <Hoffman.ElSegundo@Xerox.com> 29 Mar 89 14:15:09 PST (Wednesday)

A short note in the `Los Angeles Times' 27 March 1989 carried this summary of information from a letter in the 'New England Journal of Medicine':

#### VIRUS HITS HOSPITAL COMPUTERS

A "virus" infected computers at three Michigan hospitals last fall and disrupted patient diagnosis at two of the centers in what appears to be the first such invasion of a medical computer, it was reported last week.

The infiltration did not harm any patients but delayed diagnoses by shutting down domputers, creating files of nonexistent patients and garbling names on patient records, which could have caused more serious problems.

"It definitely did affect care in delaying things, and it could have affected care in terms of losing this information completely," said Dr. Jack Juni, a staff physician at the William Beaumont Hospitals in Troy and Royal Oak, Mich., two of the hospitals involved. "It was pretty disturbing."

If patient information had been lost, the virus could have forced doctors to repeat tests that involve exposing patients to radiation, Juni said. The phony and garbled files could have caused a mix-up in patient diagnosis, he said.

"This was information we were using to base diagnoses on," said Juni, who reported the case in a letter in the New England Journal of Medicine. "We were lucky and caught it in time."

### Prank Virus Warning Message

Bruce N. Baker <BNBaker@KL.SRI.COM> Tue, 28 Mar 89 08:06:39 PST

An individual placed a time bomb message on a government service system in the San Francisco Bay Area saying, "WARNING! A computer virus has infected the system!" The individual is learning that such a prank is considered almost as funny as saying that you have a bomb in your carry-on luggage as you board a plane.

Bruce Baker, Information Security Program, SRI International

#### Subversive bulletin boards

Eric Percival <eric%hpqtdla@hp-sde.sde.hp.com> Mon, 27 Mar 89 13:27:32 BST

This week's (26 March.) Sunday Times (UK) has an article relating to a Bulletin Board being run by a 14-year-old boy in Wilmslow, Cheshire, England, which contains information relating to such things as making plastic explosives. Anti-terrorist detectives are said to be investigating for possible breaches of the Obscene Publications Act. Apparently reporters were able to easily gain access to this bulletin board and peruse articles on such subjects as credit card fraud, making various types of explosive, street fighting techniques and dodging police radar traps. One article was obviously aimed at children and described how to make a bomb suitable for use on "the car of a teacher you do not like at school," which would destroy the tyre of a car when it was started. The boys parents did not seem to think that their son was doing anything wrong, preferring him to be working with his computer rather than roaming the streets. A London computer consultant, Noel Bradford, is quoted as having seen the bulletin board and found messages discussing "how to crack British Telecom, how to get money out of people and how to defraud credit card companies. Credit

card numbers are given, along with PIN numbers, names, addresses and other details "

## UK Computer Threat Research Association

"David.J.Ferbrache" <davidf@cs.heriot-watt.ac.uk> 28 Mar 89 09:32:34 GMT

For those of you interested an umbrella organisation has been established in the UK to co-ordinate information on, and research into all aspects of computer security. In the first instance one of the organisations primary concerns will be combatting the threat posed by computer viruses by acting as a clearing house for virus information and control software.

Below is a copy of an initial letter mailed to prospective members:

The Computer Threat Research Association

The computer threat research association, CoTra is a non-profit making organisation that exists to research, analyse, publicise and find solutions for threats to the integrity and reliability of computer systems.

The issue that caused the formation of CoTra was the rise of the computer virus. This problem has since become surrounded by fear, uncertainty and doubt. To the average user the computer virus and its implications are a worry of an unknown scale. To a few unfortunates whose systems have become a critical issue.

The key advantage of CoTra membership will be access to advice and information. Advice will be provided through publications, an electronic conference (a closed conference for CoTra's members has been created on the Compulink CIX system) as well as other channels such as general postings direct to members when a new virus is discovered.

CoTra membership will be available on a student, full or corporate member basis. All software that is held by CoTra that enhances system reliability, such as virus detection and removal software, will be available to all members. It is intended to establish discounts with suppliers of reliability tools and services. A library of virus sources and executables and other dangerous research material will be made available to members who have a demonstrable need.

A register of consultants who have specific skills in the systems reliability field will be published by CoTra and reviews of reliability enhancing software will be produced.

Your support of CoTra will ensure that you have the earliest and most accurate information about potential threats to your computer systems.

CoTra, The computer threat research association, c/o 144 Sheerstock, Haddenham, Bucks. HP17 8EX

Part of the organisation's aim is to establish reciprocal links with other similar organisations worldwide to facilitate the sharing of experience and rapid flow of information on new threats.

To this end if you are involved in, or have contacts with, a similar organisation in your country, please write to CoTra (or by email to me, and I will forward your correspondence) outlining your organisation and its aims.

Yours sincerely,

Dave Ferbrache, Dept of computer science, Heriot-Watt University, 79 Grassmarket Edinburgh, UK. EH1 2HJ Tel (UK) 031-225-6465 ext 553 UUCP ..!mcvax!hwcs!davidf

#### Will the Hubble Space Telescope Compute?

Paul Eggert <eggert%stand@twinsun.UUCP> Tue, 28 Mar 89 14:57:02 PST

M. Mitchell Waldrop's article (\_Science\_, 17 March 1989, pp 1437-1439) on SOGS is notable for its coverage accessible to the general scientific public, and for its claim that the software engineering community has switched to rapid prototyping. Selected quotes follow.

-- Paul Eggert, Twin Sun Inc. <aerospace.aero.com!twinsun!eggert>

Will the Hubble Space Telescope Compute?

Critical operations software is still a mess--the victim of primitive programming methods and chaotic project management

First the good news: two decades after it first went into development, the \$1.4-billion Hubble Space Telescope is almost ready to fly....

But now the bad news: the Space Telescope Science Institute in Baltimore still has dozens of programmers struggling to fix one of the most basic pieces of telescope software, the \$70-million Science Operations Ground System (SOGS).... It was supposedly completed 3 years ago. Yet bugs are still turning up ... and the system currently runs at only one-third optimum speed.... If Space Telescope had been launched in October 1986, as planned at the time of the Challenger accident, it would have been a major embarrassment: a superb scientific instrument crippled by nearly unworkable software....

#### [chronology:

]

```
    1980-1 2"-thick requirements doc. written by NASA-appointed committee
    1981 contract awarded to TRW; peak team included 150 people
    1983 first software components delivered
    later SOGS declared utterly unsuitable.
```

The problem was basically a conceptual one. NASA's specifications for SOGS had called for a scheduling algorithm that would handle telescope operations on a minute-by-minute basis.... The tacit assumption was that the system would schedule astronomers on a monthly and yearly basis by simply adding up

thousands upon thousands of these minute-by-minute schedules.

In fact, that tacit assumption was a recipe for disaster.... The number of possible combinations to consider rises much faster than exponentially.... In the computer science community, where this phenomenon has been well known for about 40 years, it is called "the combinatoric explosion." Accepted techniques for defusing such explosions call for scheduling algorithms that plan their trips with a road map, so to speak. And SOGS simply did not have it.

In addition to performance issues, however, SOGS was also deficient in basic design terms. "SOGS used last-generation programming technology," says one senior programmer.... "SOGS was designed in such a way that you couldn't insert new releases without bringing down the entire system! For days!" says the science institute's associate director for operations, Ethan Schreier.... Indeed, the fundamental structure of SOGS is so nonmodular that fixing a bug in one part of the program almost invariably generates new bugs somewhere else....

So, where did SOGS go wrong?...

One of the main villains seems to have been the old-line aerospace industry approach to software development.... In the wider computer science community this Give-Me-The-Requirements approach is considered a dismal methodology at best... Modern programming practice calls for ... a style known as ``rapid prototyping''...

Even more fundamental ... few people at NASA were even thinking about telescope operations in the early years.... the Space Telescope project as a whole was saddled with a management structure that can only be described as Byzantine.... At the hardware level the chaos at the top was reflected in a raft of independently developed scientific instruments and onboard computers, none of which were well coordinated with the others. Indeed, the presumption was that any such problems would be taken care of later in the software....

So, is SOGS fixed now?

Maybe. With TRW's help, the institute has spent the past several years beating the system into shape.... On the other hand, such progress has come at a price. SOGS now consists of about 1 million lines of programming code, roughly ten time larger than originally estimated. Its overall cost has more than doubled, from \$30 million in the original contract to roughly \$70 million....

In both NASA and Pentagon contracting, the cost of the old-line approach is becoming all too apparent. Indeed, it has become a real sore point in the computer community.

"it's the methodology that got us to Apollo and Skylab," says [James] Weiss [data systems manager for Space Telescope at NASA headquarters]. "But it's not getting us to the 1990s. The needs are more complex and the problems are more complex."

"SOGS," he says, "is probably the last example of the old system."

#### The Airbus disaster and Ada

<jpff@maths.bath.ac.uk>
Wed, 29 Mar 89 11:03:08 BST

This is a question for RISKS. I found this on the network. Can any RISKS-readers answer it?

From: bob@imspw6.UUCP (Bob Burch) Newsgroups: comp.misc,comp.lang.ada Subject: French Airbus Disaster / Ada? Date: 27 Mar 89 12:37:11 GMT Organization: IMS, Rockville, MD

I am hearing a couple of versions of the role which the Ada programming language might or might not have played in the air-bus disaster at the Paris Air Show about a year or so ago. I would appreciate hearing from anyone who actually knows anything about this topic.

Ted Holden, HTE

#### ✓ DIAC-90

Douglas Schuler <douglas@atc.boeing.com> Wed, 29 Mar 89 08:08:18 pst

Call for Papers
DIRECTIONS AND IMPLICATIONS OF ADVANCED COMPUTING
DIAC-90 Boston, Massachusetts July 28, 1990

Computer technology significantly affects most segments of society, including education, business, medicine, and the military. Current computer technology and technologies that seem likely to emerge soon will exert strong influences on our lives, in areas ranging from work to civil liberties. The DIAC symposium considers these influences in a broad social context - ethical, economic, political - as well as a technical context. We seek to address directly the relationship between technology and policy. We solicit papers that address the wide range of questions at the intersection of technology and society.

Within this broad vision, we request papers that address the following suggested topics. Other topics may be addressed if they are relevant to the general focus.

#### RESEARCH DIRECTIONS DEFENSE APPLICATIONS

- + Research Funding Sources/Effects + AI and the Conduct of War
- + Software Development Methodologies + Autonomous Weapons Systems

COMPUTING IN A DEMOCRATIC SOCIETY COMPUTERS IN THE PUBLIC INTEREST

+ Community Access + Computing for the Disabled

+ Computerized Voting

+ Uses of Models and Simulations

+ Civil Liberties

- + Arbitration and Conflict Resolution
- + Computing and the Law
- + Computing in Education
- + Computing and Workplace
- + Software Safety

Submissions will be read by members of the program committee, with the assistance of outside referees. The program committee includes Alan Borning (U. WA) Christiane Floyd (Technical University of Berlin), Jonathan Jacky (U. WA), Deborah Johnson (Renssalaer Polytechnic), Eric Roberts (DEC), Richard Rosenberg (SIGCAS, U of British Columbia), Ronni Rosenberg (MIT), Marc Rotenberg (CPSR), Douglas Schuler (Boeing Computer Services), Lucy Suchman (Xerox PARC), and Terry Winograd (Stanford).

Complete papers should include an abstract and should not exceed 6000 words. Papers on ethics and values are especially desirable. Reports on work in progress or suggested directions for future work as well as appropriate surveys and applications, will also be considered. Submissions will be judged on clarity, insight, significance, and originality. Papers (4 copies) are due by March 1, 1990. Notices of acceptance or rejection will be mailed by April 15, 1990. Camera ready copy is due by June 1, 1990. Send papers to Douglas Schuler, Boeing Computer Services, MS 7L-64, P.O. 24346, Seattle, WA 98124-0346. For more information contact Doug Schuler (206-865-3226).

Proceedings will be distributed at the symposium, and will be available during the 1990 AAAI conference. The DIAC-87 and DIAC-88 proceedings are published by Ablex Publishing Company. Publishing the DIAC-90 proceedings is planned.

Sponsored by Computer Professionals for Social Responsibility P.O. Box 717, Palo Alto, CA 94301

DIAC-90 is partially supported by the National Science Foundation under Grant No. 8811437, through the Ethics and Values Studies Office.



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 8: Issue 47

Saturday 1 April 1989

## **Contents**

- Summary of recent news briefs on "hacker" activity <u>Anonymous</u>
- "Free Fall" -- new book on 1983 Air Canada near-disaster **Rich Wales**
- Farm worker killed by conveyor

**Walter Roberson** 

Hackers dictionary in Japanese?

Les Earnest

- Undetected Monitoring Programs and Privacy Rights Donald B. Wechsler
- Re: Ada and Airbus

John Knight via A. Blakemore and Mike Linnig

Galactic Hacker Party

Rop Gonggrijp

- Virus in PKARC software
  - Bob Kozlarek via Robert Casey via A-N-Onymouse
- Computer Documentation Course Queries

Stephen W. Thompson

Info on RISKS (comp.risks)

#### Summary of recent news briefs on "hacker" activity

<[Anonymous]>

Sat, 1 Apr 89 00:00:00 -0000

March 17, Newsweek: "I Must Set A Proper Example." Interviewed on the MacNeil-Lehrer show yesterday, the president's nominee for head of the Office of the War on Addiction said that if confirmed he will abstain from use of his private Macintosh while he is in office.

March 19, Wall Street Journal headline story: "HTH International announces \$20M Initial Stock Offering, opening a new chain of hacker treatment homes."

March 20, AP, Murray Hill, NJ: At a meeting of Hackers Anonymous last

evening, well-known computer scientist C.A.R. Cudder declared, "I am a hackaholic."

March 23, San Francisco Chronicle: The head of one of the largest insolvent savings and loan institutions (having lost \$6 billion, with evidence of substantial internal fraud) attributed its demise to "malicious hacker activity by holders of student loans".

March 24, Raleigh Times: RJ Reynolds Co today withdrew its newest product, the Hackerette. A spokesman explained that it features a program filter that delivers a hacking-equivalent jolt with no provably harmful side-effects. The filter had apparently been infected by a tobacco virus.

March 25, Charleston Gazette: In his weekly sermon, a noted TV evangelist sharply condemned Hackers Anonymous for distributing sanitized workstations to confirmed hackers. He declined to comment on the new interactive video game, Satanic Nurses.

March 27, Los Angeles Times: Interviewed on a corner at Rodeo Drive yesterday, the former first lady offered her advice to teen-age hackers: "Just say Logoff!" One block away, a street vendor offered the reporter an updated map of the movie stars' homes including modem phone numbers and passwords.

March 28, CBS News: A notorious hacker, convicted of fraud earlier in the week, was released with a suspended sentence. He denied that it was he, using his one post-arrest phone call, who had transferred \$500,000 from the municipal court's traffic-fine account into the judge's personal checking account.

Number 1 on the NY Times best-selling book list for the week ending March 31: The Six-Week Program-All-You-Want Crash Cure for Hacking, published by Hackers Anonymous.

April 1: According to advance promos, on 'Nightline' tonight a noted TV evangelist will admit to Ted Koppel that he paid a hacker to demonstrate computer intrusion in his motel room.

[Several items from the National Enquirer and the Weakly Whirled News were low on credibility, and have been omitted from this compendium. By the way, in general I do not like to accept anonymous messages, unless for some reason it is essential to protect the author or his/her associations; furthermore, anonymous messages should have a higher level of accuracy and precise references than attributed contributions -- although ALL authors should follow the masthead guidelines. PGN]

#### "Free Fall" -- new book on 1983 Air Canada near-disaster

Rich Wales <wales@CS.UCLA.EDU> Fri, 31 Mar 89 16:49:02 PST

The April 1989 \_Reader's Digest\_ contains a condensed version of a new book, \_Free Fall\_. The subject is Air Canada Flight 143 (23 July 1983) from

Ottawa to Edmonton, which came extremely close to becoming a major disaster when the airplane (a Boeing 767) ran completely out of fuel while in the air.

The problem resulted from a combination of circumstances:

- (1) Both the electronic sensor designed to measure the fuel supply, and its backup, failed, and the necessary replacement parts were not readily available. This meant that the crew had no direct indication in the cockpit of their fuel status; the fuel gauges were dependent on the plane's computer equipment and were thus blank.
- (2) A "dipstick" procedure for measuring fuel supply by hand was done incorrectly, leading the mechanics to conclude that the plane had more fuel than was in fact the case (and, thus, that it was safe to fly the plane without working fuel gauges!). The error was later traced to the fact that the airplane was one of the first Canadian 767's built to metric specifications -- and the mechanics had committed a simple math error because they were still used to measuring fuel in pounds instead of kilograms.

Further, when the plane finally ran completely out of fuel and both engines failed, the entire instrument panel -- now bereft of electrical power -- went blank. The radar transponder also failed, making it impossible for air traffic controllers to track the plane. Fortunately, an older radar facility in Winnipeg was still operational, enabling some degree of tracking from the ground.

Fortunately as well, the pilot of the now powerless and instrumentless 767 had had extensive experience as a gliding instructor. He managed to land the jet -- without engines -- at an abandoned military airstrip about 50 miles north of Winnipeg. Although a small fire broke out in the plane, it was quickly extinguished. No one (either in the plane or on the ground) was killed or seriously injured; the plane, however, narrowly missed hitting several people camped on or near the long-abandoned runway. The plane sustained moderate damage, primarily because the nose gear did not extend all the way to its "locked" position and collapsed on landing; but it was eventually repaired and still flies today.

Air Canada initially laid the blame on the pilot, co-pilot, and maintenance workers (the pilot had at one point tried to help the struggling ground crew with the fuel calculations, but ended up making the same math error). Eventually, though, a board of inquiry commissioned by the Canadian federal government overturned this ruling and cited Air Canada's rush to introduce a new aircraft that weighed fuel in kilos (while older planes continued to use pounds), without giving adequate training to the maintenance personnel, as the major cause of the accident. Both pilot and co-pilot received numerous awards for the skills they displayed in saving Flight 143, and both continue to fly airplanes for Air Canada.

My reporting of this story is not intended as a condemnation of the metric system. Indeed, I myself have long been a staunch advocate of metrication. But the RISK of confusion and error attendant with conversion to a new and unfamiliar system of measurement -- coupled with the

RISK of depending on advanced electronic systems that leave one little or no manual recourse if they should fail -- deserves note.

-- Rich Wales // UCLA Computer Science Department // +1 (213) 825-5683 3531 Boelter Hall // Los Angeles, California 90024-1596 // USA wales@CS.UCLA.EDU ....!(uunet,ucbvax,rutgers)!cs.ucla.edu!wales

### Farm worker killed by conveyor

<Walter\_Roberson@carleton.ca>
Thu, 30 Mar 89 22:24:29 EST

Tuesday (March 28), a 16 year old farm worker was killed "when he was caught between a conveyor belt and a doorframe." The details aren't clear from the article, but the article does say that an electrical breaker, a plug, a kill switch, and a direction control were all within the worker's reach at the time he was killed. The worker's overalls became snagged on the chain-type conveyor, which was only moving at one foot per minute. The implication from the article seems to be that the youth had never been taught how to turn off the machine!

Walter Roberson < Walter\_Roberson@Carleton.CA>

[There have been several computer/robot-related deaths in the past. This one gets included as a "related system" (see masthead) and the necessity of being trained to copy with exceptional situations. PGN]

#### Hackers dictionary in Japanese?

Les Earnest <LES@SAIL.Stanford.EDU>
30 Mar 89 2155 PST

I received an off-the-wall phone call last night from an editor who is overseeing the translation of the Hackers Dictionary into Japanese. That amusing compilation was put together a decade or so ago by A.I. grad students at Stanford, MIT, and Carnegie-Mellon and recorded the then-current vernacular of their shared cultures. They did it for fun, but it somehow ended up getting published.

The Hackers' Dictionary contains more than a few puns, jokes, and other things that are hard to translate such as "moby," as in "moby memory", or "fubar" and its regional variants "foo bar" and "foo baz". While a Japanese version of this dictionary might be of some limited value to a person who comes to the U.S. for an extended visit, there are clearly some risks involved in attempting such a translation.

The particular problem that prompted the call was the definition of "logical." Apparently the dictionary gives as an example a statement something like "If Les Earnest left and was replaced by another person, the latter would be known as the logical Les Earnest." This had been written when I was the principal bureaucrat of the Stanford A.I. Lab. and was apparently intended to describe

some set of responsibilities that could be transferred from one person to

The editor reported that the Japanese translator had been hopelessly confused by this example; he found "earnest" in the dictionary but was unable to figure out what a "Les Earnest" was. The editor had tried to explain it to him but was unable to get the idea across. He finally called me to find out what my official job title had been, so that he could describe the example in more generic terms.

I hope that they manage to work it out, but I am not willing to bet that the Japanese Hackers Dictionary will be fully comprehensible.

Les Earnest

[If he were Less Earnest, this would have been Less Interesting. PGN]

### Undetected Monitoring Programs and Privacy Rights

Donald B. Wechsler <m17434@mwvm.mitre.org> Friday, 31 Mar 1989 18:14:17 EST

PC WEEK (March 27, 1989) reports:

"The recent rash of remote local area network software packages has thrust the PC industry into a national controversy over electronic monitoring and workers' rights to privacy.

At question is whether or not products such as . . . Microcom Inc.'s Carbon Copy, which can be configured to allow undetected monitoring of PCs, violate workers' Fourth Amendment rights 'of people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures.'

In answer to complaints from Massachusetts unions that workers' rights are being violated, the Massachusetts Coalition of New Office Technology (CNOT) plans to set up some guidelines to regulate employers who opt for electronic monitoring. The group's first step is to file a bill with the Massachusetts Dept. of Labor that would force employers to notify job applicants of any electronic monitoring . . . and to inform workers when they are being monitored."

Carbon Copy is usually perceived as software which allows one PC to be controlled from another remotely located one. But programs like Carbon Copy can be configured to observe network activity without a user's permission, detection, or override. Lisa Morel of Microcom reports that: "the ones who are asking about it [undetected monitoring] are the system managers."

While monitoring software can provide important network trouble- shooting and

tuning help, users may view its secret operation as "condoned tapping." Monitoring differs from event logging. More than recording what the user does, monitoring software clones the user's activity on the observer's terminal.

Interest in using undetected monitoring programs may increase with growing concern about network security and management. These programs are not limited to PC platforms. Moreover, serious reservations reach beyond the nasty business of how managers gather employee performance data.

- o The observer may monitor user access to organizationally sensitive information.
- o Secret monitoring conflicts with the Information Resource Management (IRM) principle of user data ownership.
- o From a lay legal view:
  - In a Federal government environment (including contractors), secret monitoring of user access to personnel information could lead to violation of the Privacy Act of 1974 (Public Law 93-579).
  - Undetected monitoring of a third-party's remote session could violate the Electronic Communications Privacy Act of 1986 (Public Law 99-508).

In efforts to preserve security and integrity, are system managers and their parent organizations prepared to handle the ramifications of secret monitoring?

## ★ Re: Ada and Airbus (Let's not start any stupid rumors) [RISKS-8.46]

linnig@skvax1.csc.ti.com>
Thu, 30 Mar 89 12:10:58 CST

From: blakemor@software.ORG Newsgroups: comp.lang.ada

Subject: Re: Ada and the airbus disaster

I am forwarding this reply from John Knight at SPC -- AB

Ada has not been used in any AIRBUS system that I know of that is in production. It has been used to develop a shadow AIRBUS flight control system to evaluate Ada. The system turned out very slow so they used a faster CPU to ensure meeting deadlines (actually, 4 times faster).

[However, stay tuned for an update on the Air France Airbus A-320 story, expected to be published in this country on 2 April. PGN]

#### Galactic Hacker Party

ROP GONGGRIJP <rop@neabbs.UUCP> Thu Mar 30 02:00:20 1989

**GALACTIC HACKER PARTY** 

2nd, 3rd, 4th of August 1989
PARADISO, AMSTERDAM, HOLLAND

During the summer of 1989 the world as we know it will go into overload. An interstellar particle stream of hackers, phone phreaks, radioactivists and assorted technological subversives will be fusing their energies into a media melt-down as the global village plugs into Amsterdam for three electrifying days of information interchange and electronic capers.

Aided by the advanced communications technology to which they are accustomed, the hacker forces will discuss strategies, play games, and generally have a good time. Free access to permanently open on-line facilities will enable them to keep in touch with home base -- wherever that is.

Those who rightly fear the threat of information tyranny and want to learn what they can do about it are urgently invited to interface in Amsterdam in August. There will be much to learn from people who know. Celebrity guests with something to say will be present in body or electronic spirit.

The Force must be nurtured. If you are refused transport because your laptop looks like a bomb, cut off behind enemy lines, or unable to attend for any other reason, then join us on the networks. Other hacker groups are requested to organize similar gatherings to coincide with ours. We can provide low-cost international communications links during the conference.

For further information, take up contact as soon as possible with:

HACK-TIC PARADISO

P.O. box 22953 Weteringschans 6-8
1100 DL Amsterdam 1017 SG Amsterdam
The Netherlands The Netherlands

tel: +31 20 6001480 tel: +31 20 264521 / +31 20 237348

fax: +31 20 763706 fax: +31 20 222721

uucp:..!mcvax!neabbs!rop fido: 2:280/1 Hack Tic telex: 12969 neabs nl

# ✓ Virus in PKARC software

<portal!cup.portal.com!A-N-Onymouse@unix.SRI.COM>
Fri, 31-Mar-89 03:44:01 PST

The following was posted on USENET:

From: rfc@briar.philips.com (Robert Casey;6282;3.57;\$0201)

Newsgroups: rec.ham-radio,rec.ham-radio.packet

Subject: virus in PKARC software

Message-ID: <47960@philabs.Philips.Com>

Date: 27 Mar 89 14:34:24 GMT

Date-Received: 28 Mar 89 14:49:14 GMT Sender: news@philabs.Philips.Com

Organization: Philips Laboratories, Briarcliff Manor, NY

copied from packet:

Date: 25 Mar 89 03:56:53 UTC (Sat)

From: wa2sqq@kd6th.nj.usa.hamradio (BOB

WARNING! WARNING! WARNING!

From: WA2SQQ Bob Kozlarek

Subject: Software Virus PKZIP/PKUNZIP .92 AM40/AM41

Recent developments in the software world have required the famous PKARC software to be replaced by a new version called PKZIP/PKUNZIP.

While several versions have been seen, the latest appears to be version .92 . Usually listed on landline BBS's is a program which will provide a menu driven screen for PKZIP, usually listed as AM-40 or AM-41.

After running these one time, the embedded virus allocated 13 meg of memory to "never never land". It appears that this "strain" looks to see how much memory is occupied on the HD and then proceeds to gobble up an equal amount of unused memory. The results are devastating if you have more than 50% of the drives capacity in use. With the assistance of Gary WA2BAU I was able to retrieve the lost memory by using CHKDSK /f. For those of you who are not familiar with this DOS command, drop me a line @KD6TH and I'll elaborate. My sincere thanks goes out to Gary WA2BAU for saving me lots of disk handling! Please pass this on to your local BBS and be sure to include the remedy.

Best 73 de WA2SQQ, Bob Kozlarek, @KD6TH in Wycoff, NJ

# Computer Documentation Course Queries

"Stephen W. Thompson" <thompson@a1.quaker.in> Thu, 09 Mar 89 13:53:13 -0500

Considering the dangers of using software and hardware for which doc is poor, I think that the following, found on a distribution list I receive, is very appropriate for this list. Certainly RISKS readers are likely to have many good suggestions, and a discussion of how we may improve how we create/use/misuse documentation would be, to me, quite useful. Responses to Joel's query go, of course, directly to him, but I'd think that discussion can go to RISKS. (Subject to the usual RISKS guidelines and our moderator's opinion, of course.)

```
> February 14, 1989
                      SCUP@TUFTS.BITNET
                                                VOLUME 3, NUMBER 5
    A service of the Society for College and University Planning
      Edited by John A. Dunn, Jr., Vice-President, SCUP
>
> Institutional Planning Office, Tufts University, Medford, MA 02155
>
        COMPUTER DOCUMENTATION COURSE QUERIES
> Joel Kahn, Southwest Missouri State University (JCD715T@SMSVMA)
>
>I am working on a proposal to add to the curriculum here a course in
>writing computer documentation. The course, as currently envisioned,
>would deal with both hardware and software docs, and would focus
>primarily on satisfying the needs of the non-technical end-user. The
>course would be offered by the English department but might be included
>in the degree programs of other departments such as Computer Science,
>Communication, etc.
>In order to provide evidence for the need for this course, I'm
>gathering information on the attitudes of users toward the state of
>computer documentation today. Anyone who would like to assist me can
>do so by answering the following questions:
>
>1) On the usual scale of F to A, what overall grade would you give
> to the docs you've used over the past few years?
>
>2) What is/are the most common, persistent, and/or destructive
> problem(s) you've encountered in these docs?
>
>I would also be grateful if anyone who has had direct experience with this kind
>of course -- as teacher, student, whatever -- would give me useful advice.
I sent Joel mail asking for permission to submit his guery to RISKS.
His response is also thought provoking.
>Date: 9-Mar-1989 09:13am EST
>From: JCD715T@SMSVMA.BITNET
>Subject: Documentation Survey
>Dear Steve,
>
>I would be pleased if you would forward my docs survey to RISKS and to
>any other lists that you think might be suitable. In addition, I would
>like to start gathering data on this through the SnailNet, for a number
>of reasons that I won't go into here. The vital info:
>Joel Kahn
>534 E. Grand
>Springfield, MO 65807
>Please circulate this address to any and all interested parties,
>especially people connected with magazine and book publishing.
>I think I'm onto something big here, something that goes far beyond
>one course at one school. I seem to have tapped into a great wellspring
```

>of anger and frustration, and the material I've gathered should be good >for at least an article, if not a whole volume. > >I thought you might be interested in an interim summary of the results, >so here it comes. >Overall average grade: C-. (Personally, I think they were too lenient.) >Most common complaints (in no particular order): > Inability by writers to see non-technical end-user's viewpoint; > > Lack of GOOD examples; Lack of good index or any index at all; IBM in general. [....] > > >Usual disclaimers: SMSU bears no responsibility for anything in this >letter; results are totally unscientific and informal; use only as >directed; your mileage may vary; etc, etc, etc. . . . Joel Kahn >

Stephen W. Thompson, 215-898-4585 Institute for Research on Higher Education University of Pennsylvania, Philadelphia, PA 19104

----- End of Forwarded Message



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 8: Issue 48

Monday 3 April 1989

## **Contents**

BMW's DWS system

**Brian Randell** 

Risks of insomnia

Roger H. Goun

VDT Risks? No, Lead pipe cinch.

F. Baube

Aircraft running out of fuel in flight

**Dale Worley** 

Yet another round of Airbus A320 discussions

Joe Morris

Daylight savings change requires computer shutdown

Walter Roberson

Elevator accident kills 13 year old

Walter Roberson

Re: "Free Fall" -- new book on 1983 Air Canada near-disaster

**Henry Spencer** 

Newspapers' computer access to public records

Wm Randolph Franklin

Computers and Property Revaluation: It's Great in Dayton, Ohio

John Karabaic

Credit card magstripe-encoded pictures

**Brian Randell** 

Using Pre-release Software

David A. Honig

Computer say, go to jail

**Clifford Johnson** 

Accidental erasure of magnetic media used by the public

**Peter Jones** 

Info on RISKS (comp.risks)

#### 

Brian Randell <Brian.Randell@newcastle.ac.uk> Sat, 1 Apr 89 12:11:13 BST

Today's Independent newspaper contains an advert by BMW which provides yet further evidence of the automative industry's flagrant disregard for the possible risks associated with new computer-based technology. The main text of the advert is reprinted below, in its entirety, followed by a brief note of some of what I regard as the more obvious risks.

#### BEFORE A BMW WILL START IT WEIGHS UP WHO'S DRIVING

First BMW brought you ABS, for safer braking in the wet. Then came ASC, to help counter wheelspin during acceleration. Today, they can unveil DWS: probably the most significant advance in anti-theft technology to occur in recent years.

DWS stands for Driver's Weight Sensor. A unique system that compares the driver's weight with a pre-programmed value stored in the sensor's computer memory. If the two values do not match, the car simply refuses to start.

Clearly, this represents a whole new level of anti-theft sophistication. But one that has only be made possible thanks to recent advances in space satellite PHAT technology. This remarkable new material - Poly Halide Anodal Tritium - exhibits a highly predictable change in electrical conductivity according to the pressure exerted upon it. By harnessing these properties, BMW's engineers have devised a wafer-thin pressure pad that, when incorporated into the driver's seat, can electronically assess the occupant's weight to within 10 grams accuracy.

Such is the system's intelligence, it will take account of bodyweight variations that occur according to the time of day, or even the time of year. This it achieves by interlocking with the car's on-board 365-day digital clock. Accurate allowance can then be made for weight increases that may be expected immediately after meal times, and those that are caused by multi-layer clothing during the winter months.

Despite its space age technology, the operation of DWS is simplicity itself.

On entering the car, the driver inserts the ignition key, at which point the words 'Code Enter' flash up on the dashboard LED display. Up to five of these codes can be stored for five different drivers. The driver now enters his personal code on the key pad and his weight appears on the light-up display, expressed in either pounds or kilos. (Lady drivers who would prefer this visible display switched off should consult their BMW dealer, who will carry out the small necessary adjustment free of charge.)

The sensor weight reading is then compared to the programmed weight in the memory, and providing this falls to within +-5%, the car will start normally. If, however, the figure exceeds these tolerances, then a discreet gong sounds, and the entire ignition system shuts down.

Should persistent attempts be made to restart the car, an alarm system is triggered, and the headlights flash alternately until the unauthorised person vacates the seat and re-closes the door.

At the same time a pre-recorded message is transmitted on the standard

police radio frequency, notifying all walkie-talkie equipped police officers within 350 metres of the car's registration number.

If you'd like to know whether the Driver's Weight Sensor anti-theft system can be fitted to your car, contact your local BMW dealer, or post off the coupon below [to Hugh Phelfrett, BMW Information Service, PO Box 46, Hounslow, Middlesex, TW4 6NF].

Some likely risks:

Just when you have arrived back from a week-end backpacking, and are desperate to get to MacDonald's before they close, the car is likely to refuse to recognise you. (The opposite problem is perhaps not so bad - for example, it would be good for you to be occasionally forced to walk or jog to WeightWatcher's class.)

Suppose the car does consent to take you to MacDonald's, the weight display, which I assume is dynamically updated, will be an additional and dangerous distraction while you drive home eating your Big Mac. (A head-up display would reduce this risk.)

A person's weight variations over the year are strongly correlated to cultural, racial, and religious factors. Almost certainly, therefore, this system will provide another example of "computerized discrimination".

There is even a security-related risk. By periodically dieting, a spy could use the occasional transmissions of the pre-recorded message as a covert signalling channel to a near-by embassy, say.

Brian Randell, Computing Laboratory, University of Newcastle upon Tyne JANET=Brian.Randell@uk.ac.newcastle UUCP =...!ukc!newcastle.ac.uk!Brian.Randell PHONE = +44 91 222 7923

### Risks of insomnia

Roger H. Goun <goun%evetpu.DEC@decwrl.dec.com> 30 Mar 89 14:04

From The Wall Street Journal, Thursday, March 30, 1989, p. A1:

"DIAL-A-SNORE: People having difficulty sleeping can dial the Lenox Hill Hospital Sleepline in New York. An answering machine plays an eight-minute tape that includes a message designed to help insomniacs doze off while listening."

Pity the poor insomniac who does fall asleep in the middle of such a call:

- After eight minutes, the Lenox Hill Hospital answering machine will hang up and a loud, synthesized telephone company voice will say, "If you'd like to make a call, please hang up and try again."
- If our insomniac manages to sleep through that, his or her phone might

well remain off-hook all night, blocking incoming (possibly emergency) calls.

-- Roger Goun

#### ✓ VDT Risks ? No, Lead pipe cinch.

"F.Baube" <fbaube@note.nsf.gov> Sun, 02 Apr 89 17:11:54 -0400

There has been mention of a high incidence of miscarriages at the headquarters of USA Today in Rosslyn, Virginia. The cause was suspected to be VDT usage.

The Washington DC \_City Paper\_ of March 31 states that the cause has since been determined to be lead in the buildings pipes.

## Aircraft running out of fuel in flight

Dale Worley <worley@compass.com> Mon, 3 Apr 89 11:44:32 EDT

This is quoted from memory from a Wall Street Journal article on the event: The manufacturer's "minimum equipment list" for the 767 includes two electronic fuel guages. Thus, technically, the pilot took the plane off with inadequate equipment. I can understand why both the pilots and the airline would consider manually measuring the fuel level with a dipstick to be fully equivalent to the electronic fuel guage, but this event shows that one should probably fly by the book; infrequently performed manual backup activities have a high likelihood of error.

Dale Worley, Compass, Inc.

#### ✓ Yet another round of Airbus A320 discussions

Joe Morris (jcmorris@mitre.arpa) <jcmorris@mitre.mitre.org> Sun, 02 Apr 89 18:45:44 EST

This morning's Washington \_Post\_ has a near-full-page article on fly-by-wire aircraft and the safety issues involved. It's a rather well-written piece which (unlike too many of the so-called "news" reports) is not written to prove that the FBW systems ("are absolutely safe"|"are not at all safe"). Choose your favorite ending; both types of "news" are available.

(The article is on page C-3; issue date is Sunday, 2 April)

The article cites the Airbus crash in France last 26 June. That crash has been the subject of numerous RISKS submissions which have explored many of the issues, but the \_Post\_ article cites other Airbus problems I haven't seen detailed. They include "...engines unexpectedly throttling up on final approach; inaccurate altimeter readings; sudden power loss prior to landing; steering problems while taxiing."

The reports are credited to "the European press". Can anyone elaborate on the reports?

[Nancy Leveson is in DC this week, and picked up a copy. If no one else comes up with a fuller report, Nancy has promised one for Tuesday night. PGN]

## ✓ Daylight savings change requires computer shutdown

<Walter\_Roberson@carleton.ca>
Sun, 02 Apr 89 13:52:18 EST

I found this on one of the systems I use (not the one I'm mailing from.) The times involved match exactly with those from previous time changes, so I begin to suspect they're serious about how long it takes.

Walter Roberson

VM/CMS downtime

-----

NEWS DOWNTIME provides information about scheduled and unscheduled shutdowns as well as extended crashes. [...]

---- 89.03.02 0800 - 89.03.02 1300

On Sunday April 2 1989 VM/HPO will be down from 0800 to 1300 hours and TSS and MVS/XA will be down from 0800 to 1000 hours for the change to Daylight Saving Time.

#### Elevator accident kills 13 year old

<Walter\_Roberson@carleton.ca>
Sun, 02 Apr 89 14:29:56 EST

The following was extracted from The Ottawa Citizen, Sunday April 2, 1989, pg A1 + A2:

Elevator accident kills 13-year-old refugee (By Dennis Foley, Citizen staff writer)

A 13-year-old girl [...] was crushed to death Saturday in an Ottawa apartment elevator that residents say has a history of malfunctioning.

Segal Samanter jumped on the elevator and was caught between the closing door and the door frame [...] She was crushed against the upper door frame.

Several residents said all three elevators continually malfunction and passengers are often jarred by their quick-closing doors. [...]

"If they break down, they're repaired immediately," he said. "There was an elevator repairman here today." [building manager, Cliff Gray]

He didn't know which of the three elevators had been repaired Saturday. [...]

"There is always something wrong with these elevators. They move when they're not supposed to, and they stop between floors." [Afshin Adill]

Ababdihakim Ali, 19, said that earlier in the day the door of the elevator in which Samanter was killed would close only halfway. It continued to operate this way, he said. [...]

Witnesses said the elevator had stopped several centimetres above the floor level before Samater (sic) got on.

Awleker Ahmed, 16, said he had been standing alongside Samanter in the elevator lobby and had warned her against trying to jump on to the elevator, which already contained several passangers.

She ignored his warning, he said. [...]

Pat Baerg, the building's secretary, said problems with the elevators are the result of tenant abuse.

"If children didn't play on them and tenants didn't jam the doors open with cardboard, we wouldn't have problems," she said.

She also said many tenants didn't know how to properly use them.

"It's a tenant problem, not an elevator problem," she said. [...]

#### ★ Re: "Free Fall" -- new book on 1983 Air Canada near-disaster

<attcan!utzoo!henry@uunet.UU.NET> Sat, 1 Apr 89 22:06:32 -0500

>(2) A "dipstick" procedure for measuring fuel supply by hand was done

- > incorrectly, leading the mechanics to conclude that the plane had
- > more fuel than was in fact the case (and, thus, that it was safe to
- > fly the plane without working fuel gauges!)...

Does the book (or the condensed version) address the question of whether this "safe" procedure violated regulations? My recollection of what was said at the time is that it's okay to fly a 767 with both fuel gauges operating, and it's okay to fly with one gauge operating plus the dipstick check, but if both gauges are out [as in the 1983 case], the plane is supposed to stay on the ground, period.

Whether my memory is correct or not, taking off with no fuel gauges strikes me as a dangerous and foolhardy action. Quite apart from reducing a redundant system to a single failure point (the manual calculation), the decision to take off without gauges also quietly assumed that nothing would go wrong in such a way as to quietly reduce available fuel (e.g. a leak). The real problem here was not unit conversion, but the old "it can't happen to me" syndrome. Bet that pilot never takes off without gauges again, ever, dipstick tests or no dipstick tests.

Henry Spencer at U of Toronto Zoology

#### Newspapers' computer access to public records

Wm Randolph Franklin <wrf@mab.ecse.rpi.edu> Mon, 27 Mar 89 15:58:10 EST

Some newspapers in the area are trying to obtain magtape copies of public records that already available on paper, such as driver licenses, criminal

convictions, and land ownership. They want to perform statistical tests and cross-database matching. This would seem to have all the dangers of governmental database matching, e.g. that when a coincidence is found, the victim is assumed guilty and must prove his innocence.

However, the newspapers might be harder on an innocent victim than the government since they can publish anything, however false, if they can't be proved to have been malicious. Finding and printing an interesting coincidence, perhaps that you own property next to someone accused of organized crime, and also sold your previous car to another organized crime suspect, wouldn't be malicious, just sensationalistic.

Wm. Randolph Franklin, RPI

#### Computers and Property Revaluation: It's Great in Dayton, Ohio

John Karabaic <fuzzy%aruba.dnet@wpafb-avlab> Fri, 31 Mar 89 08:52:31 EST

From an informational notice entitled "Important Answers about PROPERTY REVALUATION" hung on my doorknob by a representative of the Montgomery County Auditor's Department (Dana A. Stamps, County Auditor):

... [previous Important Answers, to questions like {\bf What is the purpose of a revaluation program}]

{\bf How is my property value determined}

In the first phase, data collectors -- who are not appraisers -- verify and update the County property data file by making an on-site visit to your property. Using the information gathered by the data collector and sales data from the local market, the appraiser uses a computer to perform statistical analysis and mathematical calculations necessary in arriving at two basic approaches to value for residential property -- the Cost Approach and the Market Approach -- to compare your property to the current market trends and assist him in his final conclusion of value.

The computer then produces an appraisal review card, from which a professional appraiser will determine the actual value in a final field review of each parcel. All final value conclusions are made by an experienced appraiser during this review. With the laborious tasks of statistical analysis and calculations being done by computer, the appraisers are now free to concentrate their talents on evaluating the results. Through integration of the electronic efficiency and accuracy of the computer with the experience and sound judgement of professional appraisers, the auditor's office will save the taxpayers of this county many thousands of dollars on future revaluations and enhance the quality of the appraisal process. ... [more Important Answers follow]

No news yet on any systems acquisition fiascos in the Auditor's Office, but the tone of the letter shows that the Auditor expects

county property owners to sleep easy knowing that their tax bills are being set with the help of "the electronic efficiency and accuracy of the computer." There is an appeal and review process for individuals, but no mention of how the statistical model itself is validated. {\em Quis custodiet ipsos custodes}?

Lt John S. Karabaic (fuzzy%aruba.dnet@wpafb-avlab.arpa) WPAFB, OH 45433-6543

## Credit card magstripe-encoded pictures (RISKS-8.45)

Brian Randell <Brian.Randell@newcastle.ac.uk> Tue, 28 Mar 89 12:48:06 BST

Regarding Mike Trout's query:

>But on a more important topic, is there any empirical >evidence to suggest that credit card fraud could be significantly reduced by >facial images, either true photographs or digitized images?

Several years ago I was told by the late Charles Read, who at the time was Director of the Inter-Bank Research Organisation, here in the UK, that they had run an experiment on the use of photographs on credit cards, as an aid to reducing fraud. He told me that: "We sent out a dozen people, each with a credit card bearing the same photograph of the same gorilla, and on average they succeeded in passing the card eight times!" (I found the phrase "the same photograph of the same gorilla" particularly memorable, and have often wondered what the results would have been if they had used different gorillas!)

Brian Randell, Computing Laboratory, University of Newcastle upon Tyne

#### ✓ Using Pre-release Software

"David A. Honig" <honig@BONNIE.ICS.UCI.EDU> Sun, 02 Apr 89 15:20:45 -0700

April's IEEE Spectrum contains an article about the design of the Intel i860 (aka "N10") RISC processor. In a section called "Unauthorized Initiative" [p 26] the author (T. S. Perry) includes the following story:

One of the designers heard from a friend in Intel's CAD department about a tool that would take a design from the logic-simulation level, optimize the circuit design, and generate an optimized layout. The tool eliminated the time taken up by circuit schematics, as well as the checking for schematic errors. It was still under development, however, and while it was even then being tested and debugged by the 486 team (who had several more months before deadline than did the N10 team), it was not considered ready for use.

The N10 designer accessed the CAD department's mainframe through the in-house computer network and copied the program. It worked, and the bus-control bottleneck was solved.

Said CAD manager Nave guardedly, "A tool at that stage definately has problems. The specific engineer who took it was competent to overcome most of the problems himself, so it didn't have any negative impact, which it could have. It may have worked well in the case of the N10, but we don't condone that as general practice."

A number of classic RISKs are apparent, but what stands out to me is the lucidity in the last paragraph and the importance of engineers' \*understanding\* their tools, not just \*using\* them. (This also reminds me of how some mathematicians get upset when they perceive engineers using mathematical tools without a good understanding of their basis, e.g., using integration without studying measure theory first...) Of course, it is not just electrical engineers but social `engineers' and other planners, controllers, etc. that need to understand their tools functions and limits.

## Computer say, go to jail [Re: Driscoll, RISKS-8.44]

"Clifford Johnson" <GA.CJJ@Forsythe.Stanford.EDU> Wed, 22 Mar 89 15:52:49 PST

Same problems in Silicon Valley. I rear-ended a car in stop/go traffic in December (my first ever collision). I gave the guy I hit my insurance details, and reported the matter to my insurance, who agreed to pay, no problems.

A month later I got a notice that my license would be suspended in two weeks for being in an accident and not having insurance. I was informed that after that date I would be automatically jailed if any officer caught me driving. How did the State hear of the accident, and how did it conclude I was uninsured? I've no idea. The telephone number they gave was \*permanently\* busy, I tried many times, but I \*immediately\* had sent them documentation which proved I had been insured.

Two months later I got a notice informing me that my suspension had been cancelled, after it had been in place for some weeks. I'm glad I wasn't stopped during that time is all I can say.

## Accidental erasure of magnetic media used by the public

Peter Jones <MAINT@UQAM.BITNET> Thu, 30 Mar 89 12:10:48 EST

I noted with interest the article on the erasure of floppy disks placed vertically behind a child's car seat in an automobile equipped with seat heaters. I wonder if the data was made unreadable by the magnetic field of the heater, or if the disk was raised to above the Curie temperature (the point where a substance loses its magnetism because of thermal agitation.)

Today, there was a bulletin on the radio in which the Montreal Urban Community Transportation Commission (MUCTC), the authority that operates the buses and subway (Metro) in Montreal, announced a problem with the magnetic stripe at the bottom of its monthly passes when used in automatic turnstiles. They claim

that some six hundred of the five hundred thousand issued monthly (0.12%) are damaged by proximity to magnetic latches in purses and wallets.

Does anyone know if credit cards are subject to this problem?

Peter Jones MAINT@UQAM.BITNET (514)-282-3542



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 8: Issue 49

## Wednesday 5 April 1989

## **Contents**

- An unusual "common mode failure" in B-1B aircraft
- Gripen crash caused by flight control software Mitchell Charity Mike Nutley
- Airbus A320 article plus some comments **Nancy Leveson**
- Info on RISKS (comp.risks)

#### ★ An unusual "common mode failure" in B-1B aircraft

Peter Neumann < neumann@csl.sri.com> Wed, 5 Apr 1989 10:44:35 PDT

A rather bizarre common mode failure has been detected in the recent inspection of grounded B-1B bombers: there was a shortage of lubricant in a critical gearbox in 70 of the 80 planes inspected (with 17 more still to go). The problem was found on the plane whose wing swept into the fuel tank (RISKS-8.46), which resulted in two shafts fractured and a leak along a fuel tank seam. [San Francisco Chronicle, 5 April 1989, p. A7]

## Gripen crash caused by flight control software

<mcharity@ATHENA.MIT.EDU> Wed, 5 Apr 89 01:15:31 EDT

(quotes&inserts from FLIGHT INTERNATIONAL, 25 March 1989)

On Feb 2 the 1st prototype (of 5) of Sweden's Saab JAS39 Gripen fighter crashed on landing after its 6th test flight. It impacted, broke left main gear, bounced, skidded and flipped.

"Gripen is naturally unstable and has a triplex digital fly-by-wire system

with a triplex analogue backup."

Initial flight was "some 18 months behind schedule" and this was "attributed to difficulties in proving the software for the flight control system."

After the 1st flight, test pilot ``remarked that the control system seemed too sensitive and that the control laws would probably need to be changed." On all flights ``the aircraft experienced problems with lateral oscillations." [On the] ``last flight oscillation in pitch was also apparent."

The accident investigation committee chairman ``confirms earlier assumptions that the flight control system was at fault."

#### Chairman:

"The accident was caused by the aircraft experiencing increasing pitch oscillations (divergent dynamic instability) in the final stage of landing, the oscillations becoming uncontrollable. This was because movement of the stick in the pitch axis exceeded the values predicted when designing the flight control system, whereby the stability margins were exceeded at the critical frequency."

Separate investigation by the JAS Industry Group:

"The control laws implemented in the flight-control system's computer had deficiencies with respect to controlling the pitch axis at low speed. In this case, the pilot's control commands were subjected to such a delay that he was out of phase with the aircraft's motion."

"the company hopes to fly JAS39-2 before the end of the year."
"Delivery of the first production aircraft [...] is now expected in [1993, although typo said '1933'], instead of 1992."

#### Swedish Gripen Fighter Crash

<jpff@maths.bath.ac.uk>
Wed, 5 Apr 89 17:09:44 BST

From Datalink, April 3 1989 (a British paper for system/software) quoted in full without permission.

Swedish wind cuts fly-by-wires

Flight-control software has been blamed for the crash of the prototype Swedish Gripen fighter last February. The preliminary report from the Swedish government's crash-investigation commission indiffied the software's inability to cope with gusting winds and the oversensitivity of the control system as the prime reasons for the accident.

According to a spokesman for the commission, problems with the \pound 3.2 billion project first arose in an earlier flight test. "The preceding test flight had shown up problems, but it's not a problem with the aircraft or with the flight control systems. It's a software problem.

"The whole of the control system was too sensitive for the pilot; it operated too fast. It was too easy for the pilot to go outside the flight-control envelope into unstable flight."

In common with many fighters currently being developed, the JAS39 Gripen is designed to be inherently unstable to increase its manoeuverability. It relies on the software to keep it under control.

"There were limitations on the flight control systems, but during the landing phase the wind was stronger than allowed for by these limitations. The pilot had to try to overcome them."

A final report into the crash is due in May, but work has already started on the second prototype aircraft, including a modified version of the flight-control software.

Mike Nutley

## Airbus A320 article plus some comments

<levesonelectron.LCS.MIT.EDU>
Wed, 05 Apr 89 13:54:29 -0400

Here is the full Washington Post article, interspersed with a few of my comments.

WASHINGTON POST: OUTLOOK, 04/02/89 Copyright (c) 1989 The Washington Post Co. By Jim Beatson

[Jim Beatson writes on aviation issues for the Guardian and some other British newspapers. He is currently living in Canada. NGL]

[Apparently either Beatson or the Post removed some more controversial items from the original British appearance of this material. PGN]

IN JUNE, a new plane hits the American skies. Northwest Airlines will become the first U.S. carrier to take delivery of the European Airbus A320 -- the most advanced passenger aircraft in the world, and already one of the most controversial. In use since last May by British Airways and Air France, the medium-sized 150-seat twin-engine jet is the first airliner to have every function, from flight controls to toilet operation, directed by computer.

On June 26, 1988, two days after the third A320 went into service, it crashed while performing a low-level pass at a French air show. A woman and two children on board were killed. An investigation blamed the accident on pilot error, but the pilot faulted a number of factors including the aircraft's computers for providing incorrect altitude information. (The pilot, a senior Air France captain, was subsequently dismissed.) Since then, various unsettling reports have appeared in the European press, regarding: engines unexpectedly throttling up on final approach; inaccurate altimeter readings; sudden power loss prior to landing; steering problems while taxiing.

[NGL: It is interesting that the pilot was never believed about the altimeter although there is not plenty of evidence to back up his story. I have noticed several things about evaluation of

#### accidents in general:

- 1) Human error is always the first ascribed cause whenever a human is involved in the system where an accident occurred. However, most accidents are multi-factorial. If the altimeter is indeed inaccurate, then the accident was only partially caused by the pilot. Humans tend to want simple answers to complex problems and to be able to ascribe blame to some single cause. There are, of course, other factors at work in these oversimplifications such as liability issues and misplaced faith in technology. But seldom are accidents the result of only one thing going wrong. Actually, the few times I have found this to be true (i.e., one thing is at fault), it is a computer that is the primary agent. Perhaps engineers expect other things to fail and therefore design systems so that a single failure cannot lead to an accident. But since (as engineers often tell me or write in system safety evaluations) computer software does not fail...
- 2) If a human cannot be blamed, then the hardware is. The first incident involving the Therac 25 occurred in Hamilton, Ontario. The accident was blamed on a faulty microswitch (a "transient" failure since nothing could be found wrong with the microswitch). The fix for the problem was to put in a duplicate microswitch to detect when the filter was not in place to correctly filter the X-ray beam. When the next incident occurred in Tyler, Texas (again involving the misalignment of the filter), it was believed that the burn suffered by the patient (who died from his injuries 6 months later) was electrical. Nobody believed that he could have suffered an overdose or that the computer could be involved. The electrical system was checked out and found to be OK so the machine was deemed safe. Two weeks later another man was overdosed in Tyler (he died two weeks after this) and FINALLY, someone (at the hospital) decided the computer might be involved. It was the physicist at the hospital who was able to reproduce the problem and raise an alarm about the computer. He had some difficulty convincing anyone else about this. The Therac 25 victim in Georgia had great trouble convincing anyone that the Therac was responsible for her severe burns. This was true also for the first overdose in Yakima. Finally, when the second person was overdosed in Yakima (and all the prior incidents had occurred including the detection of an error in the software that could have caused the incidents), people were willing to examine the possibility that this was a software error (a different software error was given the blame this time). Why are people so reluctant to believe that the computer may be at fault?]

[returning to the Washington Post article]

Of course, the introduction of any new aircraft entails shake-out problems of one kind or another. But the A320's extensive use of computers raises a new set of questions: Are we ready to rely so heavily on complex software systems for such safety-critical applications as commercial flight?

#### Bird on a Wire

The control system employed by the A320 is known as "fly by wire." FBW replaces the conventional stick and rudder controls with a series of computers and miles of electronic cables. Instead of the familiar control-column, the pilots use "side-sticks," a single lever resembling the joy sticks used in video games.

Sensing devices which gauge the aircraft's flight characteristics pass the information to the six color monitors that replace nearly all the traditional analog instruments and result, Airbus says, in 75 percent fewer instruments than conventional configurations. On the uncluttered flight deck, the pilot on the right uses the side-stick with the right hand while the pilot on the left has a left-handed version. (On the left, pilots tend to push the aircraft to the right owing to the position of the forearm and wrist; that side-stick was adjusted to compensate.) But the computer system actually directs the control surfaces. Only the rudder and horizontal stabilizer -- both on the tail -- be mechanically directed by the pilot.

All other flight controls are managed by the electrical flight-control system (EFCS), which contains three spoiler/elevator computers (SEC), two elevator/aileron computers (ELAC) and the flight-augmentation computer that oversees stability, limiting and protection functions. The engines and throttles are managed by the full-authority digital engine-control (FADEC) computers. The EFCS uses "dissimilar redundancy." That is, computers that are designed to back each other up are of different brands, have different microprocessor types and are supplied by different vendors -- all to minimize the likelihood of identical hardware parts failing at the same time. And different programmers were employed to write each of the parallel sets of software. Moreover, each computer is divided into two physically separate units with "segregated" power supplies.

[NGL: There were different programmers. Were there different requirements specifications? How about design specifications? How much detailed design information was provided to the programmers?]

The EFCS is designed to fly within a theoretical "flight envelope" -- permissible ranges for various maneuvers -- thus providing computer-monitored protection against windshear forces, overload or overspeed conditions. If the pilot were to, say, allow the speed to drop toward the stall point, the computer would sound alarms and automatically increase the power.

In the event that two computers should disagree, one automatically shuts itself down and its tasks are carried out by the other. For example, if one unit directed the flaps to be partly extended and its monitoring software expected full flap extension, then the first unit would automatically shut itself down and its functions would be passed over to the other. The pilots' display monitors would tell them what had happened. Finally, each of the five flight-control-surface computers is capable of performing all of the essential tasks of the others as well as its own tasks.

[NGL: If two computers disagree, how is it determined which computer

to shut down? It does not sound like the pilots do this, they are just told about the event afterward (and may not have the information necessary to make this decision anyway). So how is the decision made? How do they know that the monitor is correct and the other one is not?]

The Airbus A320, of course, is not the first civilian aircraft to use computerized control. Boeing's 757 and 767, for example, have computeractivated spoilers; and Boeing had planned to use FBW technology in the 7J7 but subsequently deferred development. Joe Sutter, Boeing's chief engineer for the past 20 years, believes that "fly-by-wire is way overstated as to its benefits"; and as for the side-stick, system, "we have some reservations -- like what one pilot is doing is not obvious to the other."

"The main benefit of FBW," he says, "is to reduce weight and increase range. It will really boost safety. But fooling around with FBW to reduce [something like] tail size goes against the design philosophy I have always urged -- that you've got to design an aircraft which one day for some reason or other is going to get into a hell of a lot of trouble. "That means mechanical back-up systems for the main control surfaces. "What happens with FBW when the aircraft gets outside its control laws? Its going to leave the pilot in one hell of a lot of trouble -- for what? One-percent fuel burn?"

A great deal more than that, says Airbus, which believes it now enjoys a significant competitive advantage over Boeing and McDonnell Douglas in fuel and weight savings. An Air France official says that the Airbus A320 is 40 percent more fuel efficient than the old Boeing 727s they have replaced. He was expecting 8 to 9 percent better, "but it's a good result anyway."

How Safe Is Safe?

But for all FBW's advantages, critics argue that its sophisticated computer system may be too far ahead of its time because of our relatively limited ability to test the reliability of software.

Airbus Industry executive Robert Alizart believes that the duplicate architecture "reduces the chances of a total system loss to an absolute minimum." But Martyn Thomas, chairman of Praxis Systems, which produces special high-reliability software for Britain's Air Force, believe such precautions offer no guarantees. "Errors get through," Thomas says. "There may be common sources of error, such as a faulty specification, which cause the same mistakes in every version of the program. Identical errors may be made by independent teams. Testing only exercises a small proportion of the possible situations that the program may have to handle."

Peter Neumann, a computer scientist at S.R.I. International, a Menlo Park, Calif., think tank, is a specialist in software engineering who has documented hundreds of software failure cases in the aerospace and other industries. Neumann says, "There are very serious risks in reliance or software in safety-critical applications. A seemingly innocuous addition to the software could have disastrous effects not discovered in testing. Never trust anyone who says such failures can never happen."

The task facing testers is prodigious. "For even small amounts of software," says Thomas, "the number of possible paths far exceeds the number which could realistically be tested. For example, a recent module comprising 100 lines of

assembly code was analyzed and found to contain 38 million possible paths, of which 500,000 could be followed with valid input data."

Mike Hennell, head of Computational Mathematics at Liverpool University -- an authority on software reliability -- has not examined the A320's software code. Still, he says: "I wouldn't get into an Airbus A320 or any fly-by-wire aircraft."

"We don't have the technology yet to tell if the programs have been adequately tested. We don't know what 'adequately tested' means. We can't predict what errors are left after testing, what their frequency is or what their impact will be. If, after testing over a long period, the program has not crashed, then it is assumed to be okay. That presupposes that they will have generated all of the sort of data that will come at it in real life -- and it is not clear that that will be true."

Indeed, scientists have been working for 15 years on software reliability models, writes John Musa of AT&T's Bell Laboratories in the February issue of IEEE Spectrum. And they are now "moving into practice and starting to pay off." But they "deal with average rather than specific behavior, since the random nature of program usage and fault introduction generates failures at random." In the case of an airline reservation system, for example, "it is impossible to predict the next specific input and hence the next specific failure. Average behavior, however, can be characterized."

The international design standard for airborne software systems (RTCA DO-178A) was developed by the Washington-based Radio Technical Commission for Aeronautics. Nancy Leveson, a specialist in software safety research and currently a visiting professor at MIT, says that DO- 178A is "not adequate for certifying commercial aircraft software. It lacks any mention of formal verification of safety, as required, for example, by the Department of Defense" which demands safety and hazard analysis.

The FAA does, however, oblige developers "to use certain accepted concepts for design and development," says Mike DeWalt, an aircraft computer software specialist with the FAA. Although FAA officials do not see all the programming ("obviously there's no way in the world that a review agency could look at that much code"), they do demand adequate testing and quality evaluation, and even sample the programmers' work. "Basically, we take a slice through the whole system," says DeWalt. That is, pick a function like left aileron control and "follow it all the way down through testing and configuration management."

"I don't want to imply that manufacturers and subcontractors will not do their best," Leveson says. "After all, they have the liability, and I'm sure they are decent human beings who care about human life. The problem is that without external review, we are depending on the competence of the employees of these companies, and I am less sanguine about the general state of software engineering knowledge and practice in industry than I am about the good intentions of humans."

Daryl Pederson, deputy director of the FAA's Aircraft Certification Division and the man charged with certifying the A320, says of DO-178A, "The document recognizes that you can't test every situation you encounter." His British counterpart, Brian Perry, head of Avionics and Electrical Systems at the Civil Aviation Authority, agrees: "It's true that we are not able to establish to a fully verifiable level that the A320 software has no errors. It's not satisfactory, but it's a fact of life."

Computers in the Sky

Nonetheless, FBW offers the pilot some real gains. In extreme situations such as suddenly encountering strong windshear, the computers instantaneously compensate. Gordon Gorbes, chief test pilot for Airbus, says, "If a pilot has to make violent changes to the aircraft's attitude in an emergency, then the computer will prevent the pilot pushing it past design strengths. For example, the computer would prevent the pilot putting it into a dive that might break off the tail." And FBW saves money for the plane's owner, by reducing hardware costs, keeping the aircraft at optimum fuel-saving trim and facilitating the switch from three- to two-person flight crews.

Many pilots flying the A320 have been enthusiastic in praising its handling and flying qualities. But some have complained about software problems and control irregularities. (The number of such complaints, according to Airbus' technical director, Bernard Ziegler, is small.) One problem reported by Air France, in a memo dated July 10, 1988 to Airbus, noted a software bug in its altimeter which measures the aircraft's height, a problem which has also been observed with British Airways' A320s. It is this problem that the pilot of the A320 that crashed at the small French airport at Mulhouse last June claimed contributed to the accident.

[NGL: And which no one believed at the time.]

There are various ways to fix a bug or add to a plane's installed software. Complete boxes containing replacement hardware and software can be exchanged by Airbus Industries. For carriers like Northwest, with 100 aircraft on order, this option would be expensive. So reprogramming could take place at a keyboard in the aircraft, conducted by Airbus or Northwest engineers. With over 640 aircraft on order around the world using two different makes of engine and a variety of sub-systems, the problem of "configuration management," as it is termed in the computer industry, becomes apparent.

[NGL: Note that a configuration management problem involving a navigation computer was implicated in the Antarctica crash of the Air New Zealand plane into Mount Erebus. Of course, planes are not sent back to the factory for all of the hardware design changes that occur -- usually the maintenance crew handles them, Is the problem different for software?]

So does the problem of anticipating a near-infinitude of real-life contingencies. In 1983 a United Airlines Boeing 767 went into a four-minute powerless glide after the pilot was compelled to shut down both engines because of overheating. The National Transportation Safety Board discovered that the plane's computerized engine-management system had ordered the engines to run at a relatively slow speed to optimize fuel efficiency. In the flight's particular atmospheric circumstances, however, this had allowed ice to build up on some engine surfaces, reducing the flow of air and causing the engines to work harder and overheat.

"The problem is that the designer didn't anticipate all the possible demands the software would face," says Hennell. "The computer will always do something. But it will only do the correct thing if it has

been programmed for that situation."



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 8: Issue 50

Wednesday 5 April 1989

## **Contents**

Mechanical Horse Racing

**Mike Trout** 

Elevator death update

Walter Roberson

Re: Elevator accident kills 13-year-old

**Eric Roskos** 

Federal Pay System botch-up

**Tim Shimeall** 

NYTimes business readers shown the future

Mitchell Charity

Newspapers and access to public records

J. Eric Townsend

High-Tech Locomotives

Mark Brader

Military software

**Henry Spencer** 

Authenticating Internet mail

Peter Scott

Advertising vs the net

Brian Kantor via Skip Montanaro

Gorillas in the Missed Identification

Joe Morris

Jay Elinsky

**Eddie Caplan** 

Info on RISKS (comp.risks)

#### Mechanical Horse Racing

Mike Trout <miket@brspyr1.brs.com> 4 Apr 89 17:18:58 GMT

Over the weekend National Public Radio had a piece about a new form of sports wagering: radio-controlled mechanical horse racing. Apparently the robot horses used are miniature, which allows racetracks to be placed in smaller

areas; the "horses" also of course do not require care, feeding or jockeys. The idea is being proposed by an individual who has built a few operating prototypes.

One reporter raised the question: What is to prevent an unscrupulous bettor from interfering with or jamming the radio signals? The promoter replied that he would be using military technology that prevents jamming.

I'm sure the Pentagon will be delighted to hear that they no longer have to worry about radio interference.

Michael Trout

## elevator death update

<Walter\_Roberson@carleton.ca>
Wed, 05 Apr 89 02:17:23 EST

A small update on the death of the 13-year-old girl crushed in the elevator a few days ago:

It seems that the elevator the girl was killed in was the same one that had been 'repaired' only a few hours earlier. Also, a quote from today's story (The Ottawa Citizen, Tuesday April 4, 1989, pg A1 + A2):

"The elevator was open and she took one step inside. But she didn't take the other one because the door closed and went up." ' [Idil Adam]

(She was crushed against the upper door frame. I take it she must have been caught by the inner doors and carried upwards. No mention has been made yet of any possible reason the elevator was able to move with the doors open, or of why the usual obstruction sensors didn't cause the door to open when they started closing on her. Indeed, neither of these -questions- has been raised yet in the paper.)

## ★ Re: Elevator accident kills 13-year-old

Eric Roskos <roskos@ida.org> Wed, 05 Apr 89 11:08:56 E+

Here in our office building we have elevators with similar problems, though possibly not as dangerous. A lot of these problems seem to be due to bad software.

The elevators are "Otis Elevonic 401" elevators. They appear to be microprocessor controlled; they have voice synthesizers that announce the floors, and scrolling text displays that give advertisements about the stores downstairs, the date and time of day, etc.

They have a number of problems that I've seen thus far:

1) The sensors which are supposed to stop the door when they collide with a person do not use mechanical switches; they seem to use electronic "body capacitance" switches. These switches are often out of adjustment. On some of

the doors, the door will stop and reopen before it contacts you at all. But on several of the doors, the doors won't reverse unless you actually touch both doors' switches at the same time with your hands. Contact with a coat sleeve, or hand contact with just one door, won't work. Apparently the traditional mechanical switches were replaced with electronic switches to reduce problems of mechanical wear on the switches, without consideration that the new switches are not as reliable in the field because of this adjustment problem.

- 2) There is an evident software bug in the elevators' exception handling. If the door is held open for longer than a certain amount of time, the elevator enters an exception mode in which a buzzer begins sounding (the voice synthesizer doesn't say anything during this time), and the elevator tries to close the doors even if you are still holding them open. Sometimes when it enters this mode, the elevator badly malfunctions. It will sometimes clear all or some of the buttons that were pressed. I've been on the elevator following this exception handling when the elevator was supposed to be going down and would instead go up to a floor for which no button was pressed, stop without opening the doors, and then after a moment go down to the proper floor. It looks as if the programmer(s) didn't test this exception handling very well.
- 3) The timers for how long the door stays open, etc., seem to be implemented in software, and use a mysterious algorithm for deciding how long to keep the doors open that sometimes results in the doors closing before anyone can get on the elevator. You can never tell when the door is going to close. Sometimes it takes a long time for it to do so.
- 4) It is possible to confuse the elevator by pushing more than a certain number of floor buttons at a given time.
- 5) The elevator has a feature whereby, if you accidentally get on the elevator and intend to go up when it is going down (or if it changes direction due to a timeout before you push the button), it won't let you push the button for the floor you want to go to. You can push the button, but it won't light up, and the elevator ignores it.
- 6) The buttons are apparently polled periodically by the microprocessor. When you push the button, it lights up (apparently via a local switch) while you are holding the button down; but if you release the button before the polling has detected that you pressed it, the light goes off. The initial lighting of the button seems to have been a bad design decision, since it gives the user the incorrect impression that the button pressing has succeeded.
- 7) The buttons inside the elevator are labeled with cryptic icons. For example, at the bottom of the button panel are some buttons labeled exactly like this:

One of these closes the doors, the other opens the doors. Some elevators have a front door and a back door, and the buttons for those are labelled like this instead:

Many people seem to be confused by these icons, and when trying to stop the

door from closing for someone, will push the button that causes the door to close instead.

These are only the more evident problems. The elevators have other bugs, such as a tendency to display "Japanese" characters instead of English on the scrolling displays, to not detect the door position properly if someone stops it (causing the elevator to sit until it goes into the exception mode), and other anomalies. It appears that a lot has been implemented in software that was formerly done in hardware, and the software has not yet been well-debugged.

#### Federal Pay System botch-up

Tim Shimeall x2509 <shimeall@cs.nps.navy.mil> Wed, 5 Apr 89 09:16:01 PST

In late October 1988 the Naval Postgraduate School was ordered to switch its payroll from the Civilan Pay Branch at the Naval Supply Center in Oakland to the Navy Regional Finance Center in Washington DC. Since then, there have been hundreds of errors in paychecks reported to the comptroller's office at NPS. The conversion was almost completely botched:

- Even though the data was computerized both in Oakland and Washington, the switch was apparently done by manually keying in the data (this conclusion is based on the types of errors that were made)
- There was apparently NO cross checking done between the original data from Oakland and the data as recorded in Washington
- There were apparently NO sanity checks done on the data as recorded in Washington

In my case, they messed up my last name ("Shimeall" at Oakland became "Shimball"at Washington), changed my federal tax status and number of exemptions (from

Unmarried and 1 in Oakland to Single and 0 in Washington) and removed the deduction for state taxes (required of all California workers). My colleagues have reported errors including failure to include deductions for health insurance, multiplying payroll deductions (i.e., suddenly doubling the life insurance deduction), greatly increased or decreased number of dependents, and errors in amount of accumulated leave and sick days. According to the comptroller's office there have been about 5 edge-inches of reported errors in payroll.

I'm not certain if this changeover from Oakland to Washington involved just NPS or if it involved other facilities in Central and Northern California. Do any of the other RISKS readers have similar tales to tell?

Tim

#### NYTimes business readers shown the future

<mcharity@ATHENA.MIT.EDU> Mon, 3 Apr 89 23:29:46 EDT

In The New York Times, Monday, March 27 1989, page D15, Business section,

there was a 7 page, multicompany advertising block entitled Special Report: NETWORKING TECHNOLOGY and Applications , which included the following "article". It was accompanied by, and was undifferentiated from, several vanilla technical "articles".

Networking in the year 2000 A.D.

In the year 2000 networked computing is not restricted by regulatory, political, geographical, or psychological boundaries. No longer is it of any concern whether an MIS department can deliver a cost-effective, reliable, and high-performance network. [...]

[...perfectly networked world...]

Security is not compromised in all this openness. Imagine one small computer virus roaming through this perfect network. Imagine just one mischievous hacker taking on your identity. Imagine just one fanatical terrorist manipulating the world's information sources. Needless to say, "the network" requires absolute integrity. End-users are screened via eye, voice, fingerprint, and brainwave patters. In the year 2000, a worldwide common access control scheme allows for easy yet authorized access by end-users to both private and public sector information. This is not to say that once you are in, you are home free. Not at all! Users, as they are born, educated, employed, and retired, gain (and lose) access to information. Provisioning of network services is by valid want, verifiable need, absolute necessity, specific job function, and paid subscription.

There are no more privately operated and managed networks. Any privatization results in wasteful informational isolationism. The original concept of ISDN reaches its full technological glory and simply renders obsolete any other networking approach. Network processing grows to such gargantuan proportions that the telecomm companies of the world develop into non-profit, publicly funded United Nations' organizations that are chaged with the world's core central information resource.

Corporate data centers become purely business application resources in 2000. [...] Direct memory and CPU access is available from within the corporation and from without. Technology is replaced long before it breaks, Murphy's Law is amended. [...] Programmers are a thing of the past. [...]

#### ✓ Newspapers and access to public records [Franklin, RISKS-8.48]

J. Eric Townsend <flatline!erict@texbell.swbt.com> 4 Apr 89 13:21:02 CDT (Tue)

>Some newspapers ... perform statistical tests and cross-database matching. ...

Newspapers have been doing this for ages, they've just had to do it by hand. There are a handful of companies that sell all sorts of organized information to newspapers/media outlets.

If they can be proved to have been grossly negligent they're in trouble as well. Also, a newspaper that builds up a record of attacking "poor, innocent citizens" will be raked over the coals by the competition for attacking "upstanding citizens and readers".

>Finding and printing an interesting coincidence ...

This sort of thing has been used to crack major stories concerning: real estate dealers with racist selling practices, small town/county "accounting errors" and a handful of other problems. It's still very new to the newspaper industry (many of whom think a MacIntosh should be easier to use :-). Give it a few years to wear off, and they'll use it as responsibly as any other information gathering tool.

Check recent issues of Columbia Journalism Review, Editor and Publisher, et al. for articles on "computerized data gathering". There are people out there, in the newspaper industry, who are concerned about privacy and access to computerized information about individuals.

J. Eric Townsend

## 

Mark Brader <msb@sq.sq.com> Wed, 5 Apr 89 12:57:36 EDT

Quote out of context from today's New York Times (p.35):

"Engineers who design locomotives bristle at any notion that they are mired in a low-technology industry. Microprocessors control the operations of the latest generation of locomotives, they note..."

Mark Brader, SoftQuad Inc., Toronto, utzoo!sq!msb, msb@sq.com

#### Military software

Mon, 3 Apr 89 23:17:25 -0400

In the 6 Feb 1989 issue of Aviation Week:

Air Force Gen. Bernard P. Randolph, commander of the service's Systems Command, bemoaned the state of military software as a "huge problem" that runs industry-wide. "We have a perfect record on software schedules -- we have never made one on time yet and we are always making excuses", he said at an Air Force Assn. symposium. The general also weighed in with criticism of electronic combat [radar, countermeasures, etc. --HS] programs, calling them a "disaster". But he blamed government as well as the defense industry, saying Uncle Sam constantly changes requirements and budgets.

## Authenticating Internet mail

Peter Scott <PJS@grouch.JPL.NASA.GOV> Mon, 27 Mar 89 10:33:35 PST

In thinking about the specific problem, originally discussed here under the heading of "Faking Internet mail", of determining whether or not the From: header line is valid, I came upon the following scheme which would authenticate that a given message was sent by the specified (user,host), if you're prepared to assume that the mail software at the actual host claimed in the message is trustworthy, and if you assume no perversions of the network short of line-tapping.

The following is from the point of view of host A, receiving mail:

- 1) A connection is opened, and a mail dialog is initiated by a remote host.
- 2) In order to maintain upwards-compatibility with the current mail system, the dialog may proceed the same way that it customarily does, at the conclusion of which host A executes step 6 below and exits thereafter.
- 3) If the remote system supports this authentication scheme, it will send a special code to initiate the following authentication sequence.
- 4) Host A assigns an identification number n (say, the value of the system clock) to the mail message being received, and tells the remote host to associate the number n with this message.
- 5) The remote host sends the message and completes the connection.
- 6) A passes the message on to the user it is destined for, say X, with a header line: "Message n, not yet authenticated."
- 7) A decodes the From: line and constructs a message to send to the host, say B, specified as the original sending host. This will be a message containing special codes that talk directly to the mail servr on that machine.
- 8) A sends to B the message, which says: "I received a message, purportedly from user Y at your location, to which I assigned the identification number n. Did you send it?"
- 8) B receives the message. If it did send the message, it has kept a record in an authentication database cross-referencing

#### Advertising vs the net

Brian Kantor <bri>shian@ucsd.EDU><br/>5 Apr 89 13:30:17 GMT

California Assembly Bill AB576 (not yet passed into law) states that a person who uses a machine that electronically transmits messages or facsimiles of documents through connection with a telephone network to transmit unsolicited advertising material for

the sale of any realty, goods, or services is guilty of a misdemeanor.

The IEEE San Diego Section Bulletin (from which the above is excerpted) states that the SD-IEEE propose supporting that Bill.

Apparently this is an attempt to control FAX junkmail.

I do not have the full text of the Bill, but it seems to me that there is some possibility that it could affect the USENET (and other BBS-like) transmission of many types of messages that are currently accepted by this community. There might also be significant first-amendment issues.

Possibly other states might follow California's lead on this; some states have already enacted or considered FAX junkmail legislation. It seems to me that such a law must be drafted carefully to avoid fixing things that aren't broken.

It might well be worth your time to write for a copy of the Bill and comment upon it to your legislators. Remember that they don't read the net, so blowing smoke here won't help.

- Brian

## ✓ Gorilla pictures on credit cards [2nd Randell item, RISKS-8.48]

jcmorris@mitre.arpa <Joe Morris> Tue, 04 Apr 89 09:25:57 EST

In RISKS 8:48, Brian Randell reports an experiment in which a UK organization tested the utility of putting the holder's picture on credit cards as a theft deterrent. The "holder's" picture was that of a gorilla, but there was no problem using the card.

Is that \*really\* a valid test? Considering the number of strange things you can find on credit cards in the US (and probably other countries), and given that the merchants who accept the credit cards aren't expecting to have pictures on them as anti-theft measures, I don't find any justification for concluding that the test demonstrates a failure of the concept.

The use of the photo ID on a driver's license as a check for age for booze purchases is well-established, and if the clerk is careful will filter out some of the more obvious "borrowed" cards. Nobody claims that it is perfect, just that it helps reduce the use of other people's cards.

On the other hand, there is the famous (and possibly apocryphal) story of a WWII defence plant worker who demonstrated that the guards were not checking the picture badges...she replaced her picture with one of Hitler and wasn't ever stopped.

#### ★ Re: Credit card magstripe-encoded pictures [Randell, RISKS-8.48]

"Jay Elinsky" <ELINSKY@YKTVMX.BITNET> Tue, 4 Apr 89 10:18:05 EDT

Were photographs normally included on the credit cards used in this experiment? If not, then the store clerk would be going "beyond the call of duty" in checking the photograph. The clerk could even think that a picture of a gorilla is the issuing bank's logo. And if photos were normally used, the clerk might think that the person presenting the card is the gorilla's legal guardian, since you'd hardly expect the gorilla itself to walk up to the counter:-) The experiment might have been more valid if the cards had a photograph of a \*person\* who looked markedly different from the bearer of the card.

Jay Elinsky, IBM T.J. Watson Research Center, Yorktown Heights, NY

## ★ Re: Credit card magstripe-encoded pictures

<eddie.caplan@H.GP.CS.CMU.EDU> Tue, 04 Apr 89 14:19:49 EDT

Since the cashiers probably weren't aware that the gorilla was intended to be a form of identification, this result isn't surprising nor significant. especially now that many credit cards come with meaningless holographic images on them, like the bird-in-flight on the card i hold.



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 8: Issue 51

## Thursday 6 April 1989

## **Contents**

Valdez Autopilot

Glenn Lea

The National Weather Service automation vs. aviation

Randal L. Schwartz

Authenticating Internet mail

Jon Rochlis

Mechanical horse racing

**Brad Hutchings** 

Re: Airbus A320 article

**Dan Swinehart** 

**Robert Dorsett** 

**PGN** 

More on 1983 Air Canada near-disaster

**Rich Wales** 

ATM loss - no one believes the customer.

<u>jrl</u>

BMW Risks

Peter Kendell

BMW Road Warmers

**Dennis Vadura** 

Info on RISKS (comp.risks)

#### ✓ Valdez Autopilot

Glenn Lea <lea@compass.com> Thu, 6 Apr 89 10:51:07 EDT

from Boston Globe, Apr 6, 1989, front page story:

Use of autopilot tied to Alaskan oil spill

A computer operated autopilot aboard the Exxon Valdez may have been set by Capt. Joseph Hazelwood for a course that headed his ship toward a reef, overriding commands by the third mate and leading to the

nation's worse oil spill, according to an Alaskan newspaper.

The report in today's Anchorage Times was based on comments by the Coast Guard's chief marine investigator, Mark DeLozier.

According to the report, neither the third mate who was in charge on the bridge nor the helmsman who was steering the ship was aware that manual turns of the wheel had no effect on the rudder or the course of the ship because the automatic pilot had been set.

If confirmed, the report would explain how the outbound tanker - even under the hands of an unlicensed mate - veered 1 1/2 miles across an inbound vessel traffic lane and tore open eight cargo tanks on Bligh Reef 25 miles outside the Valdez oil terminal."

[Remainder of article concerns the cleanup and captain's arraignment.]

Was there no "AUTOPILOT" indicator?

Glenn Lea

#### The National Weather Service automation vs. aviation

Randal L. Schwartz <merlyn@intelob.intel.com> Thu, 06 Apr 89 09:11:47 PDT

[quotes are from Insight/April 10, 1989; typos from me :-)]

\_Weather Agency Maps More Efficient Service\_

The National Weather Service will be a leaner and much more automated operation in the 1990s. Under a modernization plan submitted to Congress, the National Association of Atmospheric Administration will establish a national network of 115 forecasting offices equipped with high-technology sensing, processing, and communication system. Currently, the service relies on nearly 300 local offices to collect and disseminate weather data.

Improved satellites, a national network of sophisticated Doppler radars (which allow forecasters to see inside storms) and a 1000-unit Automated Surface Observation System that collects temperature, wind speed, air pressure, and other atmospheric data will enable the service to phase out 800 jobs, reducing agency staff to some 3900. The new technological systems should allow for "earlier detection and permit the short-range prediction of destructive, violent, local storms and floods, thereby mitigating a glaring shortfall in current warning services," according to the service's plan.

As a pilot, I've been following the NWS transition from human observers to ASOS machines in the last year very carefully. While these machines report objective things (temperature, dewpoint, precip over last N hours) rather accurately (barring mechanical breakdown, etc etc), they do very poorly at

cloud cover and current precipitation. For cloud cover, an ASOS reports what is \*overhead\* (possibly modified by some recent history information, I'm not sure). This is very different from what the human observers report, which is generally a function of weather for about 5 miles around. This means one little stationary puffy at 1000 feet directly over the ASOS can be confused with a 1000 foot overcast.... quite a different situation. Humans can also include "rain ended at 24 minutes past the hour" or "frontal passage [a wind shift] at 18 minutes past the hour", which I believe the ASOS cannot do. (This is very useful to decide where the front will be farther downwind at a later time.) And how do you come up with a sensor that recognizes "blowing snow" contrasted with "blowing dust" (quite a different thing:-)?

The talk in the aviation community been rather specific on the resulting decrease in aviation safety because of the \*reduced\* information available to pilots. What gets me is that this article touts the \*advantages\* of automation. Notice the reduction in personnel: this will probably be all the human observers replaced with ASOS machines. The Doppler radars are mostly in place; the new satellites would have been there anyway; so all we are really doing is losing the "human touch".

On a local (for us Oregonians...) note: one of the human observations cut was a mountain-top observation station in the Cascades near Eugene (or Medford... I forget). This cut made headlines because the local meterologists were apalled; the station had been making continuous observations since the early part of this century, and served as a baseline for very long range weather trend information. Although other stations in the area provide similar information (which is reportedly why the station was cut), they have not been reporting for nearly as long, thus destroying their long-term-trend usefulness.

Randal L. Schwartz, Stonehenge Consulting Services

#### Authenticating Internet mail (RISKS-8.50)

Jon Rochlis <jon@ATHENA.MIT.EDU> Wed, 5 Apr 89 22:54:31 EDT

Date: Mon, 27 Mar 89 10:33:35 PST

From: Peter Scott <PJS@grouch.JPL.NASA.GOV>

if you're prepared to assume that the mail software at the actual host claimed in the message is trustworthy, and if you assume no perversions of the network short of line-tapping.

Both of these assumptions do not hold and probably never will. (Not only is line-tapping trivial and widespread, ala Ethernet sniffers, but modification, protocol and hardware address spoofing and the like is easy, if not trivial.)

-- Jon

## ✓ mechanical horse racing (Michael Trout, RISKS-8.50)

Brad Hutchings <hutching@cs.utah.edu> Thu, 6 Apr 89 09:09:10 -0600

There was a story a few weeks ago in the Wall Street Journal discussing this new concept in horse racing. The horses are \*not\* mechanical. The horses are of a smaller breed that was used to pull small carriages around the turn of the century. The jockeys \*are\* mechanical. They consist of a small piece of telerobotic hardware that can control the speed and direction of the horse. This controll is achieved using conventional reigns and a loudspeaker. These jockeys are controlled remotely by a radio control similar to that used for R/C airplanes and such.

The main reason for using the hardware-based jockeys is weight. Even the lightest human (wetware-based :-) ) jockey would slow these minature horses down to a very unexciting pace. The robot-jockeys weigh only 22 pounds and in the illustration they looked like a small tin man with arms, a racing derby and no legs. The original prototypes were developed for patrolling the perimeter of a very large ranch. To protect the rancher from thieves, the ranch perimeter was constantly patrolled by several men on horseback. In an effort to cut costs, the inventors thought of mounting a TV camera on a horse with some method of control, hence the robot-sentry/jockey was born.

The military anti-jamming technology mentioned involves the standard practice of encoding the control signals on many frequencies simultaneously (perhaps 10-100 different frequencies) to improve the odds of transmitting a signal in the presence of a jamming signal and/or noise.

As far as RISKS go, it doesn't take a leap of the imagination to conceive of this technology being used in battlefield environments. One of the most difficult problems currently facing robotics researchers is navigation and locomotion in unstructured environments. By coupling current robotic technology to biologically-based locomotion systems, this problem may be overcome for the time being. A variety of scenarios is possible for any animal that can be trained to respond to the commands of some robot. Perhaps the day may come when robots and animals will fight the actual battle while we humans sit back, joystick and beer in hand, safely directing the battle while remotely viewing the results on a CRT monitor (1/2:-)). Sounds like a new idea for a video game. (full:-)).

Brad L. Hutchings

#### ★ Re: Airbus A320 article plus some comments (Leveson, RISKS-8.49)

<Swinehart.pa@Xerox.COM> Wed, 05 Apr 89 21:58:24 PDT

With respect to the fly-by-wire issue, I think it's important to separate two concepts:

(1) Whether cables, hydraulic lines, or electrical signals, sensors, computers, and actuators translate the pilot's actions to the control surfaces

(the A320 article stated "FBW replaces the conventional stick and rudder controls with a series of computers and miles of electronic cables", as if similar amounts of cables or the equivalent were not required to accomplish the conventional method).

(2) How much additional "intelligence" is placed between the pilot and the control surfaces.

It may well make sense to replace mechanical cables by electrical or fiber-optic ones, for reasons of reducing cost, weight, and complexity, or of improving redundancy. I am confident that a system whose only function was to make this substitution could be made robust enough to equal or exceed the reliability of existing systems, especially in damage situations. For example, one could arrange to use multiple battery-powered actuators, with a radio link as a final backup even, to reduce the chances that an engine falling off would disrupt the control signals, as it did in the Chicago DC-10 accident. I believe many of the space shuttle controls include this direct mapping as a fallback.

Most of the FBW systems discussed in this forum apparently add significant processing stages between pilot input and control output, sometimes of necessity, since these aircraft are sometimes not inherently stable. Ultimately, that seems like a good idea, too, but it's a lot more complicated, since essentially it means that the computer is flying the plane. Clearly this approach deserves at least as much scrutiny as it is receiving, here and elsewhere.

#### Comment on commented Washington Post A320 report

Robert Dorsett <mentat@louie.cc.utexas.edu> Wed, 5 Apr 89 18:25:20 CDT

- > [NGL: It is interesting that the pilot was never believed about the
- > altimeter although there is [now] plenty of evidence to back up his story.

There is also substantial evidence to discredit him: the voice transcripts indicated a highly unprofessional preflight and takeoff. Normal checklist procedures were not used, and the atmosphere was too relaxed and casual. The French government leaked this data very early in the investigation, which undoubtably influenced where the general direction of the investigation was to go. As someone who has spent a substantial amount of time in airliner cockpits, I can say that the transcripts were quite horrifying in their lack of professionalism.

On the specific issue of the altimeter making a difference, the airplane was flying approximately 50 feet off the ground. At that altitude, the pilots' eyes should not be in the cockpit; the airplane's approximate altitude (or, more importantly, its relation to the trees and ground) could have been established at a glance. There's a simple rule of thumb in such cases: if an obstacle is above the horizon, you're going to run into it. This alone seems to suggest poor judgement, perhaps accentuated by the informal atmosphere in the cockpit and the "weekend fair" mentality of the proceedings.

I don't think the Mulhouse-Habsheim crash can be used to condemn functional aspects of the A320--at least, judging from the information I've seen on it. The crash is much more vulnerable to questions regarding the human-factors design of the A320 cockpit, and the validity work workload-saving automation and display formats. Considering how senior (each pilot had just over ten thousand hours, and the captain, at the time, was the head of the A320 program for Air France, with more time in type than anyone else) the crew was, one must at least consider the possibility that the cockpit design may have encouraged the atmosphere which led to the poor decisions which led to the crash.

Robert Dorsett UUCP: ...cs.utexas.edu!walt.cc.utexas.edu!mentat

## ★ Re: "not plenty of evidence to back up his story" (Leveson, RISKS-8.49)

Peter Neumann <neumann@csl.sri.com> Thu, 6 Apr 1989 9:24:41 PDT

In Nancy Leveson's Airbus commentary,

"not plenty of evidence to back up his story" should have been

[I corrected it in Robert Dorsett's quote of it, in the previous message.]

Boston's Logan Airport was fogged in on Tuesday evening, and Nancy took the train back from Washington DC. Evidently her train of thought was dominated by her thought of train.

#### More on 1983 Air Canada near-disaster

Rich Wales <wales@CS.UCLA.EDU> Wed, 5 Apr 89 23:15:34 PDT

Having gone out and bought the book, I now have some additional details about the 1983 incident in which an Air Canada Boeing 767 ran out of fuel while on a flight from Ottawa to Edmonton.

The book is \_Freefall\_, by William Hoffer and Marilyn Mona Hoffer; St. Martin's Press (New York), 1989; ISBN 0-312-02919-5; US\$17.95.

To recap, the plane's electronic fuel sensor system failed. The "fuel quantity processor" on the Boeing 767 in question used two separate, independent operating channels for redundancy. If one channel failed, the processor would ignore it and use the other. In this case, however, a cold solder joint in an inductor caused one channel to fail in an unanticipated way: instead of cutting off completely, this channel generated a reduced -- but nonzero -- signal. The fuel quantity processor was not designed to deal with such a situation, and so failed entirely.

The night before the fateful flight, a maintenance technician in Edmonton, Alberta tried unsuccessfully to find this problem. No replacement

<sup>&</sup>quot;now plenty of evidence to back up his story".

fuel quantity processor was available, but he discovered that by turning off the circuit breaker for the faulty sensor channel, he could get the fuel gauges to work. He marked the breaker with yellow maintenance tape and made a note in the plane's log book. However, his log notes seemed to make no sense and were misunderstood by the maintenance crew at Dorval Airport in Montreal; a technician there reset the breaker despite the tape over it, without noticing that he had thereby disabled the fuel gauges again.

Since the plane had left Edmonton the previous night with only one fuel sensor operational, the manual required a "drip" test with mechanical dipstick-like devices to double-check the fuel (kerosene) level. The fuel truck's gauges measured fuel \*volume\* (in litres) -- but this had to be translated into fuel \*mass\* as part of the "drip" test. The mechanics knew how much fuel the plane needed, in kilograms; but when they went to figure out how much fuel (in litres) to pump into the tanks, they mistakenly tried to convert from \*pounds\* to litres. This error was made all the easier by the fact that the conversion factor was labelled in the mechanics' reference books as "specific gravity"; the fact that the number also embodied a volume-mass conversion was completely glossed over. As I mentioned in my earlier message, the Boeing 767 in question was one of the first "metricized" airplanes in the Air Canada fleet; other planes still measured fuel in pounds, not kilos.

After the plane was refuelled, the pilot noticed that the fuel gauges were now blank. On this basis, he asserted to the maintenance people that the plane was not legal to fly according to the manuals. However, the mechanics insisted that Maintenance Control had cleared the plane and that it was OK to fly. In such a situation, the pilot could theoretically have stuck to his guns and refused to allow the plane to go -- but it was well known that "an overly cautious pilot who grounds too many flights for what others perceive as trivial reasons is likely to find himself grounded." Further, the written guidelines or "Minimum" Equipment List" for the 767 had already been revised agains and again -- and, in fact, there were three versions of the MEL book at this time (one for pilots, one for mechanics, and one for airport Maintenance Control). So, given that Maintenance Control had cleared the plane for takeoff on the basis of the fuel "drip" test, the pilot would have put himself in a potentially indefensible situation by challenging their decision on the basis of \*his\* copy of the MEL regulations.

The above details can be found in Chapter 13 of the book, starting on page 89.

So, to summarize, the mishap resulted in part from:

- (1) Inadequate design of the redundancy systems in the fuel quantity processor; it failed entirely in the face of an unanticipated \*partial\* failure of one of the two sensors.
- (2) Miscommunication between mechanics at airports in Edmonton and Montreal, resulting in the first mechanic's fortuitous "kludge" fix to the problem being unknowingly undone by the second mechanic.
- (3) Metric conversion woes in conjunction with the refuelling of the

plane -- compounded by the fact that a key mathematical factor in the calculation was labelled in such a way as to conceal its true role as a unit conversion factor between mass and volume.

(4) Ambiguous rules for minimum equipment and line of responsibility in determining whether the airplane was flight-worthy.

Rich Wales // UCLA Computer Science Department // +1 (213) 825-5683 3531 Boelter Hall // Los Angeles, California 90024-1596 // USA

#### ATM loss - no one believes the customer.

<jrl%mvuxr@att.att.com>
Wed, 5 Apr 18:28:43 1989

I recently had a "normal" bad experience with an ATM: (bank name withheld to protect the guilty - but it's a HUGE bank in Massachusetts). The machine gave me half the money I asked for, but the receipt read that it had given me the full amount. Of course, I immediately called the "help" line (which should perhaps be called the "I can't help" line), and reported the incident. I requested that they shut down the machine until they could audit it. To my surprise, they responded that, according to their carefully thought out policy, they could not shut down the machine on the basis of a single customer complaint.

Note, however, that if the MACHINE detects an operational irregularity, it shuts ITSELF down immediately, often without returning your card. I find it not only odd, but downright >risky< that the complaint from a customer is given less weight than the machine's "perception" of a possible problem. On the one hand, some software or hardware system has determined that there MAY be a problem - and this is acted on at once. On the other hand, I report an ACTUAL problem - and I find myself being ignored. This says volumes about the propensity to believe the computer at all costs: the customer "couldn't be right - the computer says so."

## ✓ BMW Risks (Re: RISKS-8.48)

Peter Kendell <mcvax!tcom.stc.co.uk!pete@uunet.UU.NET> 5 Apr 89 09:43:53 GMT (Wed)

You're quite right, Brian. BMW seem to specialise in providing RISKy technology. A few years back I bought a BMW316i on the basis of an ad in the Guardian describing its ionically-bound detergent-containing paint. You remember that it claimed to be self-washing. Well, imagine my surprise when returning to my new car after a particularly heavy thunderstorm I found that \*all the paint\* had washed off!

This is not to mention the self-inflating tyres that blew themselves up so much that the car lost half a ton in weight, requiring me to spend 300 pounds (BMW prices!) on a larger spoiler just

to keep the car on the road.

I note that the previous representative, Herr Uve Behnaad, has been replaced by a new man, Mr Phelfrett. It seems, however, that BMW policy has \*not\* changed and that the motoring public continues to be put at RISK by poorly-tested new technology.

[Comments also from Frank Wales <mcvax!zen.co.uk!frank@uunet.UU.NET>, who also noted Road Warmers, which follows. Gullible's Travels? PGN]

#### ✓ Re: BMW Introduces It's Newest Innovation: ROAD WARMERS

Dennis Vadura <dvadura@watdragon.waterloo.edu> Wed, 5 Apr 89 16:32:46 EDT

BMW INTRODUCES ITS NEWEST INNOVATION: ROAD WARMERS

Having spent the last twenty years perfecting the sports sedan, BMW has now taken up the ultimate challenge - perfecting the road.

Road Warmers are the result of twenty years of German engineering. And represent perhaps the single most important contribution to the automotive industry in the past decade.

Road Warmers employ laser technology to ensure constant road conditions. The way in which they operate is simple. Underneath the car, four pivoting convex lasers are mounted in front of each wheel. The lasers are aimed at the pavement directly in front of the tread stance. They work in tandem with five-speed turbo fans. So not only do they manage to melt snow and ice, they also dry the road of excess moisture. And virtually eliminate the need to clear your driveway during winter. Inside the car, the driver is continually apprised of the climatic conditions through BMW's onboard computer and Active Check Control. This enables the driver to set the road to a temperature that best suits their level of performance. The result is a road that never changes. Four seasons become one. And performace is assured like never before. Eventually Road Warmers will be standard on all new BMW's. But as part of a special offer, your dealer will install them on your present car free of charge.

But you should hurry. Our offer is only available April 1st, so you would be a fool to miss this one.

[reprinted from an add in Toronto's Globe and Mail, April 1st.



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 8: Issue 52

Sunday 9 April 1989

# **Contents**

Valdez follow-up...

Dean Riddlebarger

Phobos

**Bob Morris** 

Presumption of innocence -- for computers

Peter da Silva

1988 Toronto election

**Mark Brader** 

California's anti-fax-ad bill

David M. Gursky

Man bytes dog

**Charles Youman** 

Re: Elevator accident kills 13-year-old (John Luce via John)

J.G.) Mainwaring

Need DRAMs?

Mike Raffety

Cellular telephones

Steven C. Den Beste

CDC operating system has passwords in batch files

**Gerard Stafleu** 

Cornell Chronicle coverage of Robert T. Morris

Manny Farber via Dave Farber

Info on RISKS (comp.risks)

✓ Valdez follow-up... (Re: RISKS-8.51)

Dean Riddlebarger <rdr@killer.dallas.tx.us> 7 Apr 89 13:05:25 GMT

> [notes on autopilot connection to tanker spill.....]

Another newsgroup has an article today in which the author claims to have seen the following Valdez-related tale: The installation of Coast Guard radar equipment which could have been sophisticated enough to track the

errant vessel before it was too late had been deferred in order to provide more budget money for our ersatz war on drugs. Risks Digest is not the place for major social discussion on this subject, but I do find it interesting that the ebb and flow of socially-oriented politics may have ultimately had an impact on the ability of accident prevention systems to function at maximum effectiveness...

[Heated discussion on budget priorities, social effects, and morality should probably be directed to misc.headlines, alt.drugs, alt.flame, or some other social newsgroup.....:-)]

Dean Riddlebarger, Systems Consultant - AT&T, [216] 348-6863

Disclaimer: Any opinions expressed are mine. I'm sometimes quite proud of them, so I won't try to give credit to my employer or anyone else...

### Phobos

<RMorris@DOCKMASTER.NCSC.MIL>
Sun, 9 Apr 89 19:21 EDT

Forget computer risks - it should be clear by now that Phobos is inhabited and that they are willing and able to neutralize large threatening objects that are aimed at them. Just wait till they send something in return - that's when we'll really need SDI.

# Presumption of innocence -- for computers

<ficc!peter@uunet.UU.NET>
Fri, 7 Apr 89 12:54:14 -0400

There have been many messages in RISKS about people believing computers before people. They generally end with something like the following (taken from a recent message):

- > This says volumes about
- > the propensity to believe the computer at all costs: the customer "couldn't
- > be right the computer says so."

One thing to bear in mind is that the computer can be mistaken, but it can't be malicious. The computer program won't deliberately try to defraud a (bank/travel agency/government department/whatever). I would certainly hope that the bank would believe the computer over a customer with no documentation, at least until they can perform an audit.

On the other hand, of course, if you CAN document your case and they still stand by the computer... that's a whole different kettle of fiche.

Peter da Silva, Xenix Support, Ferranti International Controls Corporation.

### 1988 Toronto election

Mark Brader <msb@sq.sq.com> Thu, 6 Apr 89 22:31:24 EDT

I don't think there's been any more in Risks about Toronto's first foray into machine-counted votes. To recap the earlier items: many ballots were silently rejected by the (optical-recognition) machines because they were not cut accurately, and a demand for a manual recount was blocked because the election law required any recount to use the same methods as the original count.

The courts must have given this some precedence, because we have already had an appellate court ruling. The ruling was that it was not reasonable to enforce that provision of the law when the method itself was clearly defective. Consequently, manual recounts were held where necessary, and in one district the result actually did change.

Mark Brader, SoftQuad Inc., Toronto, utzoo!sq!msb, msb@sq.com

### California's anti-fax-ad bill...

<dmg@mitre.mitre.org>
Thu, 06 Apr 89 16:49:02 EST

In <u>RISKS 8.50</u>, Brian Kanto (via Skip Montanaro) writes about California's attempt to make sending junk mail by facsimile illegal. I wonder how legal this is. Suppose someone here in Washington sends a junk fax to someone else in California (I know, I'm assuming negligible costs for the phone call). How does California expect to prosecute someone in the District of Columbia for violating a California law while the person is in the District of Columbia?

If the law says that "a person WITHIN THE BORDERS OF THE STATE OF CALIFORNIA who uses..." it should be alright, but otherwise, there are some serious questions about infringement of interstate commerce (which is properly under the jurisdiction of the Federal Government) that need to be addressed.

Of course, this whole message begs the question "How is this a risk to society?"

David M. Gursky, Member of the Technical Staff, W-143, Special Projects Dept. The MITRE Corporation

# ✓ Man bytes dog

Charles Youman (youman@mdf.mitre.org) <m14817@mitre.mitre.org> Wed, 05 Apr 89 14:55:54 EST

This week's issue of Computerworld contains an article on page 10 that may be of interest to RISKS readers. The article is titled "Humane Society collars a chip off the old hound dog." Beginning the first week in May, the Marin (CA) County Humane Society will begin injecting

microchips the size of a grain of rice into animals up for adoption. The chip can be activated by waving a scanner over the animal's back and it results in a unique 10-digit number being displayed. The number is used to query a database that contains the owner's name. The purpose of the system is returning lost pets to their owners.

These implants have been available for a fee in clinics throughout Canada since last July. They have been used by some shelters and veterinarians on an optional basis in the U.S. since the last quarter of 1988.

The vendor of this system is International Infopet System of Agoura Hills. CA.

The relevance for RISKS? What if someone wants to use this technology as the basis for a national identity card for people.

# ✓ re: re: Elevator accident kills 13-year-old (RISKS-8.50)

J.G. <John>
7 Apr 89 13:06:00 EDT

#### FORWARDING OF A MESSAGE FROM JOHN LUCE:

I was a Software Engineer on the Elevonic 401 project (but not on the cab software that controls the features discussed).

Item 1: The sensors that are malfunctioning on the doors were viewed as unsafe by the engineers involved. However, mgt. felt the risk was small compared to the COST savings obtained by using them. 1 problem was that they needed adjustment often, but not replacement, while the older versions had to be replaced more often but were vastly more reliable while in service.

Item 2: The doors are forced close to prevent the tie-up of the elevator. Poor maintenance will cause the door bumpers to not retract the door. This is an easy upkeep and will fail only if the building has decided against a periodic maintenance plan and just calls when something breaks down. The holding open of the doors causes the car to go into 'Delayed Car' mode which takes the car out of service. When the doors are finally allowed to close, the car has to intialize itself. If it is in the lower half of the building, it will run up to initialize, and run down if in the upper half regardless of buttons pushed.

Item 3: The length of door open time is decided by the building owner and is put in to a Contract Table. The only thing for sure is that a door that opens answering a Hall Call will stay open longer than a door that opens for a Car Button.

Item 4: The number of floor buttons pushed doesn't cause the confusion of the elevator, it's the number of buttons tempered by the weight inside the car. If the weight sensors do not show enough weight (arbitrary, but effective) for the number of buttons pushed, it cancels the buttons. To

understand the implementation, the name of the module that does that is called 'KIDS'. It prevents the floor to floor runs kids like to have occur by pushing buttons and getting out of the car before the doors close.

Item 5: Design intent. If someone can't read the arrow to know which way the car is running, he shouldn't be allowed to put in a car call away from the direction it's moving.

Item 6: Unless this is OLD software, i.e. the building has not upgraded it, this is impossible to do. The scan and latch of buttons was placed in a 96 millisecond task.

Item 7: All the engineers agree with you on this, but since Otis sells to many foreign countries (including the oriental ones), this was the only recourse left open. I'm sure better icons could have been devised.

Finally, displays and voice are customer designated and maintained by the customer. If he fails to read the manual, these items will appear to malfunction.

I hope this clears it up. I firmly believe, even though I no longer work there, that Otis Elevator North America R&D had the best set of s/w people I've seen overall.

Any opinions expressed above are my own and not to be attributed to my present or previous employer.

John Luce

### ✓ Need DRAMs?

Mike Raffety <miker@porsche.UUCP> Sat, 8 Apr 89 21:02:27 CDT

From "Electronics", April 1989, page 18, news briefs:

NEED DRAMS? HERE'S ONE WAY TO GET THEM

If the shortage of dynamic random-access memories is abating, a band of armed robbers in California's Orange County hasn't heard about it. Over the past six months, at least five companies have been hit in late-night robberies, with the memory chips as the main target. The biggest haul was at Western Digital Corp. in Irvine, where two bandits forced an unarmed security guard to open a storage area and took some \$100,000 worth of DRAMs, according to authorities. The armed robberies are a new development in the DRAM shortage, they say, with previous thefts largely being inside jobs.

# Cellular telephones

<denbeste@BBN.COM>

Fri, 07 Apr 89 20:27:24 -0400

From the 4/7/89 Boston Globe:

"Some Bostonians are having the time of their lives eavesdropping onNynex Mobile Communications cellular phones. With the help of their trusty Radio Shack Portavision 55s, designed to pick up the audio portion of UHF television signals, these naughty people claim to have heard Secretary of Finance and Administration Edward Lashman discussing a press conference with his wife and Boston Mayor Ray Flynn checking in with his office. "It makes for a great day," says one listener who calls in sick at his job to spend the day with his ear pressed against the radio. "At 7 a.m. you hear the construction people complaining that their suppliers delivered the wrong stuff. At 9, it's the lawyers telling their clients how to lie in court. After noon the risque stuff starts..."

The article goes on to say that Radio Shack no longer sells that model, and that the FCC says such eavesdropping is illegal.

Steven C. Den Beste, BBN Communications Corp., Cambridge MA

## CDC operating system has passwords in batch files

Gerard Stafleu <gerard@uwovax.uwo.ca> Fri, 7 Apr 89 12:10:57 edt

CDC has a (relatively) new operating system for its Cybers, called NOS/VE (it has been around for a few years). While browsing through the tutorial manual, I came upon the section on batch jobs. It contains the following paragraphs:

To submit a batch job from your terminal, you first create a file that contains the job and then specify the name of the file in the SUBMIT\_JOB command.

The first line of the file must contain the LOGIN command. This command specifies the user name, password and family name to be used for the job, as in the following example:

login login\_user=pat password=secret login\_family=nve

So the user name and password will be sitting there together in a disk file, in plain text. I don't think I need to elaborate on the RISKs of this.

Note that the keeping of user name and password is not necessary, as the file is submitted from a terminal, where the user is already logged in.

CDC apparently noticed this at some point, and in a footnote they state: "If, for security reasons, you do not want to include your password in a file, you can use [some other command]." Nevertheless, this is just a footnote, and the first thing the users are taught about batch jobs is to put their user name and password in a file!

Gerard Stafleu, (519) 661 - 2151 Extension 6043 General E-mail address: gerard@uwovax.uwo.ca

[Of course this should not surprise you. It is unfortunately still quite common. to find embedded passwords. In many IBM mainframe systems, for example, FILE passwords are routinely stored, shared, and multiply used -- for different files. PGN]

## Cornell Chronicle coverage of Morris

"David J. Farber" <farber@dsl.cis.upenn.edu> Sun, 9 Apr 89 6:31:17 EDT

The Cornell Chronicle is the Administration's propaganda organ. As such, their coverage of the [Robert] Morris report is relatively one-sided, but since they got the report in advance, they summarized it. I'll put the last paragraph right here: Copies of the report are available from the Office of the Vice President for Information Technologies, 308 Day Hall, [area code 607] 255-3324.

CORNELL PANEL CONCLUDES MORRIS RESPONSIBLE FOR COMPUTER WORM (By Dennis Meredith, Cornell Chronicle, 4/6/89)

Graduate student Robert Tappan Morris Jr., working alone, created and spread the "worm" computer program that infected computers nationwide last November, concluded an internal investigative commission appointed by Provost Robert Barker.

The commission said the program was not technically a "virus"--a program that inserts itself into a host program to propagate--as it has been referred to in popular reports. The commission described the program as a "worm," an independent program that propagates itself throughout a computer system. In its report, "The Computer Worm," the commission termed Morris's behavior "a juvenile act that ignored the clear potential consequences." This failure constituted "reckless disregard of those probable consequences," the commission stated.

Barker, who had delayed release of the report for six weeks at the request of both federal prosecutors and Morris's defense attorney, said, "We feel an overriding obligation to our colleagues and to the public to reveal what we know about this profoundly distrubing incident."

The commission had sought to determine the involvement of Morris or other members of the Cornell community in the worm attack. It also studied the motivation and ethical issues underlying the release of the worm.

Evidence was gathered by interviewing Cornell faculty, staff, and graduate students and staff and former students at Harvard University, where Morris had done undergraduate work.

Morris declined to be interviewed on advice of counsel. Morris had requested and has received a leave of absence from Cornell, and the university is prohibited by federal law from commenting further on his status as a student.

The commission also was unable to reach Paul Graham, a Harvard graduate student who knew Morris well. Morris repotedly contacted Graham on Nov. 2., the day the worm was released, and several times before and after that.

Relying on files from Morris's computer account, Cornell Computer Science Department documents, telephone records, media reports, and technical reports from other universities, the commission found that:

- Morris violated the Computer Sciences Department's expressed policies against computer abuse. Although he apparently chose not to attend orientation meetings at which the policies were explained, Morris had been given a copy of them. Also, Cornell's policies are similar to those at Harvard, with which he should have been familiar.
- No member of the Cornell community knew Morris was working on the worm. Although he had discussed computer security with fellow graduate students, he did not confide his plans to them. Cornell first became aware of Morris's involvement through a telephone call from the Washington Post to the science editor at Cornell's News Service.
- Morris made only minimal efforts to halt the worm once it had propagated, and did not inform any person in a position of responsibility about the existence or content of the worm.
- Morris probably did not indent for the worm to destroy data or files, but he probably did intend for it to spread widely. There is no evidence that he intended for the worm to replicate uncontrollably.
- Media reports that 6,000 computers had been infected were based on an initial rough estimate that could not be confirmed. "The total number of affected computers was surely in the thousands," the commission concluded.
- A computer security industry association's estimate that the worm caused about \$96 million in damage is "grossly exaggerated" and "self-serving."
- Although it was technically sophisticated, "the worm could have been created by many students, graduate or undergraduate ... particularly if forearmed with knowledge of the security flaws exploited or of similar flaws."

The commission was led by Cornell's vice president for information technologies, M. Stuart Lynn. Other members were law professor Theodore Eisenberg, computer science Professor David Gries, engineering and computer science Professor Juris Hartmanis, physics professor Donald Holcomb, and Associate University Counsel Thomas Santoro.

Release of the worm was not "an heroic event that pointed up the weaknesses of operating systems," the report said. "The fact that UNIX ... has many security flaws has been generally well known, as indeed are the potential dangers of viruses and worms."

The worm attacked only computers that were attached to Internet, a national research computer network and that used certain versions of the UNIX operating system. An operating system is the basic program that controls the operation of a computer.

"It is no act of genius or heroism to exploit such weaknesses," the commission said.

The commission also did not accept arguments that one intended benefit of the worm was a heightened public awareness of computer security.

"This was an accidental byproduct of the evant and the resulting display of media interest," the report asserted. "Society does not condone burglary on the grounds that it heightens concern about safety and security." In characterizing the action, the commission said, "It may simply have been the unfocused intellectual meanderings of a hacker completely absorbed with his creation and unharnessed by considerations of explicit purpose or potential effect."

Because the commission was unable to contact Graham, it could not determine whether Graham discussed the worm with Morris when Morris visited Harvard about two weeks before the worm was launched. "It would be interesting to know, for example, to what Graham was referring to in an Oct. 26 electronic mail message to Morris when he inquired as to whether there was 'Any news on the brilliant

progject?'" said the report.

Many in the computer science community seem to favor disciplinary measures for Morris, the commission reported.

"However, the general sentiment also seems to be prevalent that such disciplinary measures should allow for redemption and as such not be so harsh as to permanently damage the perpetrator's career," the report said.

The commission emphasized, that this conclusion was only an impression from its investigations and not the result of a systematic poll of computer scientists.

"Although the act was reckless and impetuous, it appears to have been an uncharacteristic act for Morris" because of his past efforts at Harvard and elsewhere to improve computer security, the commission report said.

Of the need for increased security on research computers, the commission wrote, "A community of scholars should not have to build walls as high as the sky to protect a reasonable expectation of privacy, particularly when such walls will equally impede the free flow of information."

The trust between scholars has yielded benefits to computer science and to the world at large, the commission report pointed out.

"Violations of that trust cannot be condoned. Even if there are unintended side benefits, which is arguable, there is a greater loss to the community as a whole."

The commission did not suggest any specific changes in the policies of the Cornell Department of Computer Science and noted that policies against computer abuse are in place for centralized computer facilities. However, the commission urged the appointment of a committee to develop a university-wide policy on computer abuse that would recognize the pervasive use of computers distributed throughout the campus.

The commission also noted the "ambivalent attitude towards reporting UNIX security flaws" among universities and commercial vendors. While some computer users advocate reporting flaws, others worry that such information might highlight the vulernatiblity of the system.

"Morris explored UNIX security amid this atmosphere of uncertainty, where there were no clear ground rules and where his peers and mentors gave no clear guidance," the report said.

"It is hard to fault him for not reporting flaws that he discovered. From his viewpoint, that may have been the most responsible course of action, and one that was supported by his colleagues."

The commission report also included a brief account of the worm's course through Internet. After its release shortly after 7:26 p.m. on Nov 2, the worm spread to computers at the Massachusetts Institute of Technology, the Rand Corporation, the University of California at Berkeley and others, the commission report said.

The worm consisted of two parts--a short "probe" and a much larger "corpus." The problem would attempt to penetrate a computer, and if successful, send for the corpus.

The program had four main methods of attack and several methods of defense to avoid discovery and elimination. The attack methods exploited various flaws and features int he UNIX operating systems of the target computers. The worm also attempted entry by "guessing" at passwords by such techniques as exploiting computer users' predilections for using common words as passwords.

The study's authors acknowledged computer scientists at the University of California at Berkeley for providing a "decompiled" version of the worm and other technical information. The Cornell commission also drew on

analyses of the worm by Eugene H. Spafford of Purdue University and Donn Seeley of the University of Utah.

[This item also was sent to RISKS by Spaf and by Geoff Goodfellow.]



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 8: Issue 53

Monday 10 April 1989

# **Contents**

Product Recalls Due to Software Error

**B.J.** Herbison

Airliners running out of fuel in mid-flight

Jerome H. Saltzer

Good press in Flying

**Howard Gayle** 

Re: More on 1983 Air Canada near-disaster

Henry Spencer

PC causes multiuser host to drop off the network

Patrick Wolfe

Auto Risks

**Robert Dorsett** 

Risk of Living in Nova Scotia

**Matthew Wall** 

Otis elevator software

**Eric Roskos** 

Elevator Units

**Don Alvarez** 

Nuclear-powered vessels

Steve Bellovin

(Deep-seated) Presumption of innocence -- for computers

<u>ephraim</u>

Re: Authenticating Internet mail

John Labovitz

Passwords in plaintext

**Brian McMahon** 

Re: Cellular telephones

**Eric Thayer** 

**David Collier-Brown** 

Info on RISKS (comp.risks)

## Product Recalls Due to Software Error

B.J. <herbison%ultra.DEC@decwrl.dec.com>

#### 10 Apr 89 10:25

The following article on product recalls appeared in this morning's paper. Of the five items mentioned in the article, three of them cite `software error' as the reason for the recall. All three cases involve medical products.

B.J.

### PRODUCT RECALLS

by Mylene Moreno, States News Service [from The Boston Globe, Monday 10 April 1989, page 14]

WASHINGTON - The federal government announced the following product recalls last week. Unless otherwise noted, the recalls were voluntarily initiated by product manufacturers, importers, distributors or retailers. The list includes products distributed in New England and nationwide.

### Food and Drug Administration

- o Nellcor Inc. of Hayward, Calif., recalled 164 N-1000 Multi-function Monitors containing Display Software Version 1.0.7, serial numbers [...] produced [...]. The product is intended for use as an adjunct monitor of blood oxygen saturation, airway carbon dioxide and nitrous oxide gas levels by trained medical physicians. Due to software error, the monitor innacurately reports the partial pressures of nitrous oxide and carbon dioxide at altitudes of 2,000 feet or higher. Approximately 51 units, which were distributed nationwide and in Canada, remain to be corrected.
- o Hewlett-Packard Co., Andover Division of Andover, Mass., recalled 428 Hewlett-Packard brand Sonos 100 Ultrasound Imaging Systems, models 77000A and 77010A, serial numbers [...], a scanner for qualitative and quantitative echocardiography and echoradiology applications. The blood velocity may be incorrectly calibrated due to a software defect resulting in erroneous reading under certain conditions. Product was distributed nationwide and internationally.
- o Hewlett-Packard Co., Andover Division of Andover, Mass., recalled its series 77020 Ultrasound Systems and Upgrade Kit Software Part No. 77120-10051, an ultrasound scanner designed for radiology applications. Product may product incorrect strip chart recordings due to software error. 1,428 units were distributed nationwide and internationally.
- o Norfolk Scientific, doing business as Statspin
  Technologies of Norwood, Mass., recalled 539 boxes of Statspin
  Disposable Roto-Products, product number RD01, lot numbers
  [...]. The product, distributed nationwide, is used for plasma
  separation. Poor welds may cause the blood to leak at the seam
  at the lower or upper part of the rotor.

**Consumer Safety Commission** 

o The Vendo Company of Fresno, Calif., launched a voluntary retrofit program for 115,000 Vendo soft drink machines that are at least 38.5 inches wide. Vendo will install anti-theft devices in the machines to dissuade individuals from dangerously rocking or tipping the machines to obtain free products. In recent years, rocking and tipping has resulted in an increasing number of deaths and serious injuries. The public is encouraged to call Vendo at 1-209-439-1770 for more information.

# ★ Airliners running out of fuel in mid-flight (RISKS-8.48)

Jerome H Saltzer <jhs%computer-lab.cambridge.ac.uk@NSS.Cs.Ucl.AC.UK> Tue, 4 Apr 89 12:53:52 bst

The recent comments on use of dipsticks to measure aircraft fuel level when some number of electric gauges are malfunctioning prompts me to point out that use of electric gauges itself is actually one of the older examples of fly-by-wire introductions. No old-time pilot would consider taking off unless:

- He or she had personally dipped a thumb in both wing tank filler holes and verified that the tanks were topped off, and
  - 2. The sight gauges (glass tubes on either side of the cockpit in a high-wing plane) were filled with something that looked like fresh gasoline.

It took a long time for people to accept electric fuel gauges; they somehow just didn't give one the same level of confidence.

Jerry

# Good press in Flying

Howard Gayle TX/UMG <howard@strindberg.ericsson.se> Fri, 7 Apr 89 08:41:56 +0200

From an article on an airline accident in Flying, March 1989, p. 27:

Should an airplane or an engine be designed so that forgetting a single item could lead to a spurious but convincing appearance of a life-threatening malfunction---not immediately, but once the airplane is airborne and the omission has faded from memory?

Computer programmers face this kind of question constantly; they never know what the novice user will come up with, and so they design their programs to survive any kind of abuse.

### Re: More on 1983 Air Canada near-disaster

<henry@utzoo.UUCP>
Sat, 8 Apr 89 21:29:49 -0400

>(4) Ambiguous rules for minimum equipment and line of responsibility in > determining whether the airplane was flight-worthy.

Ambiguous rules, yes; ambiguous responsibility, no. Aviation regulations and laws are \*extremely\* clear on this: ultimate authority and responsibility rest with the pilot, and nobody else. Even air-traffic control is advisory only: the pilot is the judge of whether their advice is safe and should be followed, and if he does something clearly stupid because they told him to, it is legally \*his\* fault. The line of responsibility for determining flightworthiness may be confused in the middle, but the pilot is most definitely at the top. Aviation is one of the few fields where things are this clear-cut.

This is not to deny that pilots often are under a lot of pressure to get the plane to its destination on time, or that a cautious pilot may find himself in trouble with management. Or that a pilot with years of boring airliner flying behind him will tend to unconsciously assume that safety is inherent in the system, making him more willing to take chances when the heat is on.

Henry Spencer at U of Toronto Zoology

# PC causes multiuser host to drop off the network

Patrick Wolfe <pwolfe@kailand.kai.com> Sat, 8 Apr 89 02:09:33 cdt

The other day I accidentally discovered how to disrupt operations on one of our multiuser BSD UNIX hosts from an MS/DOS PC with PC/NFS. The PC was having a boot time problem where the message "use NET START RDR hostname" was being displayed.

I misunderstood the message, thinking that command was used to assign the host that performs authentication, and issued it substituting in the hostname of our Sequent Symmetry host. A few moments later people starting complaining that the Symmetry was down.

Actually, the "NET START RDR" command identifies the hostname of the PC, which it looks up in its HOSTS file to determine its IP network address. A message on the Symmetry's console explained why it was unavailable, b"Duplicate IP address on the network".

The risks should be obvious. System Managers should not be allowed to touch PCs without re-reading the manuals first. :-}

Patrick Wolfe (pat@kai.com, kailand!pat) System Manager, Kuck & Associates, Inc.

## Auto Risks [...cs.utexas.edu!walt.cc.utexas.edu!mentat]

Robert Dorsett <mentat@louie.cc.utexas.edu> Sat, 8 Apr 89 22:24:22 CDT

I didn't think I would run across something to surpass the BMW weight-dependent anti-theft system so soon, but today I received the Buick \_Dimension\_ promo disk. For those who aren't familiar with it, the Macintosh version runs a Hypercard-like slide-show (with music, sound, and animation) detailing the Buick product line. This year's disk mentions a new feature (with animated demonstrations): a "remote access" system on the Riviera and Riatta, two sports cars. Here's what they have to say:

"Remote Keyless Entry is designed to unlock and lock your car's doors and unlock the deck lid from up to a 30 foot radius. On some Buick models, you also control the interior lighting. On those with factory equipped theft deterrent systems, locking and unlocking automatically arms and disarms the deterrent system.

"One of billions of unique codes are programmed into the systems Erasable Programmable Read Only Memory (EPROM). Using 4 or 8-bit microprocessors, the system reacts to an operational code such as "unlock the doors," only after receiving a valid identification code.

"The benefits of this system are fully realized only after using it. How about identifying your car from others at night in a crowded parking lot by pressing a button, or being able to open the deck lid when approaching your car with your arms full of packages?

"The Keyless Entry System is standard on the Reatta, and is available as an additional feature on the Riviera and Electra/Park Avenue models."

[The problem with the KES is that this one is real -- in contradistinction to the BMW promos. The vulnerabilities are obviously considerable. PGN]

## Risk of Living in Nova Scotia

Matthew Wall <WALL@BRANDEIS.BITNET> Mon, 10 Apr 89 00:33 EDT

The Friday, April 7th Boston Globe ran a front-page story about an MIT graduate student whose car was marked as abandoned, towed, and compacted into a neat cube of steel in the space of four hours. It turns out the student was in my wife's department, and I have managed to confirm these facts:

Omitting the fact that the Massachusetts law allowed the car to be marked as abandoned based on the word of a neighbor, the Boston city police department and the Bureau of Motor Vehicle registration seem to be subjecting the driving public to the risk of parking your car, or at least parking a car from a foreign country. The student in question had previouslyst registered the car in Massachusetts, and had then returned home to Nova Scotia and had the car registered there. When he returned to Massachusetts,

in accordance with state law, he maintained the Canadian registration.

The towing authorities checked his Massachusetts registration information and found that the registration had expired a few years ago, which convinced them it was abandoned. The Globe article indicates they didn't bother checking the Nova Scotia registration (valid) because they would be forced to use the Interpol network, which is reserved for felonies.

The car was worth \$2500, pre-compaction. I wonder if \$2500 vandalism constitutes a felony offense?

The city of Boston is now attempting to recover towing fees, a \$250 fine for abandoing the car, and a \$110 fee for compacting the car. The student, Michael Picard, is suing the city.

The police seem to have relied quite heavily on a negative result from their computerized database -- an expired registration here, that means no valid registration anywhere, right? And they assumed that since the registration had expired, there was no point in using their address information to try to contact Picard.

Admitted that this might have happened to a double-parked chariot in Mesopotamia, but computers seem to have allowed the authorities to act thoughtlessly and destructively with impressive speed.

# ✓ Otis elevator software (Re: RISKS-8.50)

Eric Roskos <roskos@ida.org> Thu, 06 Apr 89 13:11:27 E+

> "The elevator was open and she took one step inside. But she didn't > take the other one because the door closed and went up." ' [Idil Adam]

This is really bad news, since it suggests something worse than just a malfunction. In the old mechanical elevators I've looked at closely, the latch that locked the outside door had a switch built into it. The latch consisted of a hook on the door that hooked into a hole in a metal box attached to the door frame. One surface of this hook was laminated with an insulating material covered with a plate of metal. (Thus, the plate was insulated from the hook and everything around it.) When the hook latched the door into a closed position, this metal plate would bridge two metal contacts inside the box the hook latched into, closing a circuit that allowed the elevator to move.

This was a clever design for several reasons. First, it wasn't possible for the switch to jam closed due to dirt, etc., since the bridging contact was pulled several feet away from the switch terminals by the door opening. It could get shorted by a piece of metal falling across the contacts, but they were about an inch apart, and inside the metal box. Second, if you manually reached inside the box, you would get an electric shock, which tended to discourage tampering (as well as discouraging people who were curious how the switch was constructed:-)). It appeared, if the designers had done this intentionally, that they had decided that the risk of the deterrent electric

shock was much less than the risk of the elevator moving with the doors open.

If this elevator had the same type of switch, it sounds as if maybe someone had bypassed the safety mechanism during one of the past repairs. Elevators are extremely powerful (the motors that move them are enormous, even for small elevators), and it appears that a lot of thought goes into the safety mechanisms used in them.

### Elevator Units

Don Alvarez <boomer@space.mit.edu> Mon, 10 Apr 89 09:27:44 EDT

Someone who used to work for Otis (I trashed my mbox and lost the name) just sent a very informative note in to RISKS regarding the design of Otis elevators. One point made in the letter is in error, in my opinion, and shows a common mistake of people assessing new technology. The author noted that the elevator buttons are polled in a 96 millisecond loop, and hence it is not possible for someone to push a button without the elevator noticing. The impression is that 96 milliseconds is very fast, because it is measured in milliseconds. If you restate the sentence as "the elevator only polls the buttons every 1/10th of a second," then the impression is that the exact same amount of time is very slow, because now it is measured in seconds.

When dealing with human major muscle motions (like moving your arms or walking), it is typical to see components of the motion happening at 50Hz. This suggests (but does not prove) that 10/second isn't fast enough to assure that the button press gets sensed. Better numbers come from a stopwatch -- I can start and stop a stopwatch in about 0.04 seconds (mine has separate start and stop buttons. With a one-button stopwatch, the time is generally just under 0.2 sec). My depressing two buttons independently in 0.04 seconds does not necessarily mean that I can depress and release one in 0.02 seconds (=20 milliseconds = 1/50th second), but it does mean that 1) 50Hz is a reasonable bandwidth for my fingers and 2) I can certainly depress and release a button in well under 1/10th of a second. The 0.2 second time for two presses of the same button with the same finger also indicates that 10/second isn't fast enough, since a simple division by two indicates that something is happening at 10Hz, and that 10Hz number ignores all the time I spend accelerating and decelerating my finger in between button presses. Finally, when I rode the elevator to my office this morning, I was able to press and light the button five times in a row without the button polling electronics noticing the action, indicating that in at least one elevator the polling loop is too slow.

Don't make performance decisions based on units. Make performance decisions based on performance.

-Don Alvarez

MIT Center For Space Research, 77 Massachusetts Ave 37-618, Cambridge, MA 02139 (617) 253-7457

[While we are on the subject of elevator repair people, anyone who thinks that this profession is unable to attract high quality personnel might be interested in Nick Christoffel, a self educated elevator repairman who is

was responsible for a wide variety of important contributions to tensor analysis and general relativity theory. Don]

# Nuclear-powered vessels

<smb@arpa.att.com>
Mon, 10 Apr 89 10:02:37 EDT

In an article on the fire about a Soviet submarine, the AP reports that five months ago, a reactor aboard an icebreaker in Murmansk almost melted down when a worker drained cooling water from an operating reactor instead of one that was shut down for repairs. They attribute that story to the newspaper Vodny Transport.

--Steve Bellovin

# ✓ (Deep-seated) Presumption of innocence -- for computers

<ephraim@Think.COM>
Mon, 10 Apr 89 09:34:42 EDT

Peter da Silva (ficc!peter@uunet.UU.NET) writes:

One thing to bear in mind is that the computer can be mistaken, but it can't be malicious. The computer program won't deliberately try to defraud a (bank/travel agency/government department/whatever).

He thereby illustrates just how deep-seated faith in computers can be! It's true that the computer \*program\*, lacking volition, won't deliberately defraud you, but can you say the same for the \*programmer\*?

Usually, yes. Categorically, no.

## Re: Authenticating Internet mail (Peter Scott, RISKS-8.50)

<jsl@cup.portal.com>
Thu, 6-Apr-89 22:35:41 PDT

[...] I came upon the following scheme which would authenticate > that a given message was sent by the specified (user,host)

[Peter describes a scheme where basically a receiving host delivers a given message to the destination user, then asks the sending host whether or not the message originated there. If so, another copy of the message is delivered to the destination user, with a header line stating that this copy is authenticated.]

This seems like a good idea, except from the point of view of the user who receives such mail. Assuming that this becomes the standard way of transmitting mail, a user ends up receiving two copies of every

message -- one unauthenticated, and one authenticated. (Except for the folks who always get fake mail. :-)

I think a better way would be to have the mail sent as usual from the sending host to the receiving host, but with an option to authenticate immediately. This would be done by having the sending host look at the received message, parse out the supposed sending host and user (from the "From:" line), open a connection to an "authentication daemon" on that host, and ask "did user <x> send message-ID <y>?"

If the sending host did not support authentication, the connection would fail, and the receiving host would add a header to the message stating that the message was possibly fake.

If the connection was successful, but the authentication failed (i.e., the receiving host didn't have the message ID in its database or the username didn't match up), the header would state that this was probably a fake message.

And of course if both the connection and the authentication were successful, the header would state that this was a genuine message.

The only problem I can see with this modified scheme is that mail sent through multiple hosts (for instance, on the UUCP network) would take three times as long to get to their destination.

John Labovitz jsl@cup.portal.com

## ✓ Passwords in plaintext (Stafleu, RISKS-8.52)

<BRIAN%UC780.BITNET@CUNYVM.CUNY.EDU>
Mon, 10 Apr 89 10:15 EST

May I add to the list of flagrant security violators the Hewlett Packard Corporation? Under MPE/V (the current OS for HP/3000 machines), all batch jobs must begin with a JOB card (those of you living in the late 1980s, substitute "line of text") which contains user and group passwords in plain text.

Interestingly, one of our systems programmers (who shall remain nameless) spoke of this as a FEATURE, because it allows users to submit batch jobs for other accounts!

Brian McMahon, Administrative Computing, University of Maryland

## Re: Cellular telephones

Eric Thayer <eht@cs.cmu.edu> Mon, 10 Apr 89 09:58:14 -0400 (EDT)

Steven C. Den Beste, denbeste@BBN.COM, quotes a Boston Globe story about cellular phone eavesdropping and says that the article claims that

> that the FCC says such eavesdropping is illegal.

Has the law changed? I was led to understand that the FCC does not ban the reception of any signal. Of course, banning the reception of certain signals is going to be tough to enforce anyway.

# Re Cellular Phone Encryption

David Collier-Brown <daveb@geaclib.UUCP> 23 Mar 89 01:22:39 GMT

karl@sugar.hackercorp.com (Karl Lehenbauer), commenting on the security of electronic mail quoth:

- > Cellular phone data encryption is a relatively simple matter as well. I don't
- > think we'll see any movement in that area until the users demand it, and the
- > government isn't likely to push heavily for it, a few strong proponents of
- > personal privacy in the legislature nonwithstanding.

Just for information, significant levels of encryption for cellular phone services have been considered by various vendors. I'm constrained not to comment on the details, but one vendor did speak with an associate and me about the time and cost of getting access to proper encryption devices for their product line. They were constrained to deal with an american company to do so, though, so I haven't heard anything more about it.

--dave (sometime security maven) c-b

David Collier-Brown, Interleaf Canada Inc., 1550 Enterprise Rd., Mississauga, Ontario yunexus!lethe!dave utzoo!lethe!dave@gpu.utcs.toronto.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 8: Issue 54

Tuesday 11 April 1989

# **Contents**

More on Otis 401 elevators

**Dave Horsfall** 

PC crashing network: blame the error message

**Mark Mandel** 

Election tampering and illegal surveillance

**Brad Sherman** 

Computer CAN attempt to defraud you

Peter van der Linden

Infallible Computers

**Dave Curry** 

Re: Airliners running out of fuel in mid-flight

Alan Marcum

Re: More on 1983 Air Canada near-disaster

Alan Marcum

Airbus A320 article plus some comments

**Greg Rose** 

Re: CDC operating system has passwords in batch files

Steve Lidie

NSA and Not Secure Agencies

**Curtis Spangler** 

California's anti-fax-ad bill...

Mark Mandel

Info on RISKS (comp.risks)

### ✓ More on Otis 401 elevators

Dave Horsfall <munnari!stcns3.stc.oz.au!dave@uunet.UU.NET> Mon, 10 Apr 89 17:32:22 est

At the RISK of turning this into a comp.risks.elevators forum, I have some further information on Eric Roskos' contribution:

The elevators are "Otis Elevonic 401" elevators. They appear to be | microprocessor controlled; they have voice synthesizers that announce | the floors, and scrolling text displays that give advertisements about | the stores downstairs, the date and time of day, etc.

### [Troubles deleted]

Yup - those are the ones in our building too. While I haven't noticed those specific troubles, there are others. They tend to cancel all calls when more than three are selected, but there is one idiosyncrasy that I find disturbing.

I have a little hand-held (amateur) transceiver, generating just 3 watts on 147 MHz from a "rubber duck" antenna - very inefficient. When I'm in the mood, I trigger it next to various bits of electronic equipment, just to test their RF susceptibility. Imagine my surprise when the lift doors immediately flew open (when closing), and a sepulchral voice announces "Do not be alarmed. We are experiencing a temporary malfunction."

Obviously, immunity to relatively weak RF fields was not a design issue.

I also get worried when their fancy flourescent display goes bizarre. I would hope that it is being driven by a slave computer, not the main control processor... I can always avoid the lifts, but 11 floors is a long way to climb the stairs.

Dave Horsfall (VK2KFU), Alcatel STC Australia, dave@stcns3.stc.oz dave%stcns3.stc.oz.AU@uunet.UU.NET, ...munnari!stcns3.stc.oz.AU!dave

# **✗ PC crashing network: blame the error message**

Mark Mandel <Mandel@BCO-MULTICS.HBI.HONEYWELL.COM> Tue, 11 Apr 89 11:31 EDT

In RISKS 8:53, Patrick Wolfe describes the consequences of his misunderstanding an error message on his PC. The message, "use NET START RDR hostname", was intended to mean

"Issue the command 'NET START RDR hostname', substituting the name of your PC for 'hostname'."

But he interpreted "hostname" to mean the name of the host to which the PC was connected, i.e., the network server, and the effect was to bring down a multiuser BSD UNIX host. He concludes:

- > The risks should be obvious. System Managers should not be allowed
- > to touch PCs without re-reading the manuals first. :-}

I draw a different and more enforceable conclusion:

ERROR MESSAGES SHOULD BE UNAMBIGUOUS, ESPECIALLY WHEN THEY TELL THE USER TO DO SOMETHING (or can be interpreted to do so).

Documentation is probably still the least-regarded aspect of software production and maintenance, but it's the user's key to the product.

#### -- Mark Mandel

# ✓ Election tampering and illegal surveillance

<br/><bks@ALFA.Berkeley.EDU><br/>Tue, 11 Apr 89 12:52:23 PDT

From "Eavesdropping Left and Right" in \_The Nation\_ of April 17, 1989, by Gregory Flannery, reporter for the \_Mt. Washington Press\_, Cincinnati, Ohio.

'... In 1979, [Cincinnati Bell's security coordinator James] West allegedly ordered a wiretap on lines serving vote-counting computers at the Hamilton County Board of Elections. As ballots were being tabulated on election night, the computer shut down for two hours. "About 8:30 ... election evening, Mr. West called me," [Cincinnati Bell installer and supervisor Leonard] Gates says. "He said we had done something to screw up the voting processor down there. He said, 'You must have done something wrong.'" Gates has testified that West told him the computer wiretap could be used to alter votes, but no evidence of such tampering has been produced to date ...'

The article also discusses other allegations which are part of a \$112 million dollar class-action suit accusing Cincinnati Bell of selling information gathered through illegal wiretaps on client telephone lines.

-Brad Sherman (bks@ALFA.Berkeley.Edu)

# Computer CAN attempt to defraud you

Peter van der Linden <linden@Sun.COM> Tue, 11 Apr 89 09:29:27 PDT

Apropos the recent claim that, though a computer may be wrong, it is not trying to defraud you -- I know of a system where the computer was programmed to defraud consumers.

A large pie manufacturing company introduced microprocessor-controlled production lines at the end of the 1970's. The system dispensed the appropriate weight of filling into each pie. State law allowed for human inaccuracy in pie fillings - if the pie was a "4oz" pie, the bakers were permitted to range from 3.5 to 4.5oz. The bakers were thrilled with the supreme accuracy of the new system, and set it to dispense at the lower limit instead of the nominal weight, all the time.

As far as I know this dishonesty continued unchecked, and it is permitted because the computer system allows an accuracy hitherto unobtainable.

### Infallible Computers

<davy@riacs.edu>
Mon, 10 Apr 89 14:06:24 -0700

On the subject of people taking the computer's word as infallible... did anyone else catch "Perry Mason: The Case of the Musical Murder" on NBC Sunday night?

Late in the show, after our hero Mr. Mason has figured out that his client is innocent and the witness currently on the stand is the murderer, he begins to question the witness as to his whereabouts. The questioning goes something like:

Q: Where were you on the night of the murder at 2:30am? A: In my room doing script revisions.

Q: How long were you workong on the script revisions? A: All night.

Q: You use a word processor to work on the script, right? A: Yes.

Q: Does the word processor put the date and time on the files you modify?

A: I don't know.

[Mason pulls out a directory listing from the fellow's computer...]

Q: Now, next to the file "Polly", what time is shown? A: 1:35am

Q: So you weren't working on the script during the time of the murder, you finished working on it much earlier? A: Yes.

And of course, the witness breaks down on the stand and confesses.

Now, granted, one can argue that it's "only television" or "just meant as entertainment". But judging by the idiotic things I've heard argued based on "I saw it on [fictional show of your choice]", I suspect a lot of people take this stuff as gospel...

Anyway, the show demonstrates the fallacy of assuming that since the information came from a computer, it is somehow ennobled, and nobody dares to question it. It apparently never occurred to these people that the time of day clock on the computer could have been wrong for some reason.

For example, the Compaq we have here for an Ethernet analyzer comes up with some random date and time every time we turn it on. It does not even prompt for the correct time (since we don't really care), one has to remember explicitly to set it (and we never bother). In fact, on most MS-DOS systems I'm aware of, just pressing RETURN gets you through the time/date stuff without ever having to set it correctly.

And as another example, Sun "generic" kernels come using the Pacific Standard time zone... how many people don't bother to change it, or just stuff the current time in without changing the time zone?

And as still a third example... how many systems out there use the "old" rules for daylight savings time conversions? They would have the wrong time for a week or so unless someone fixed it manually...

If I were the guy on the stand, I would have denied it all and forced Mason to prove that the time of day clock on the computer was correct at the time I last edited that file.

-- Dave Curry

# ★ Re: Airliners running out of fuel in mid-flight (RISKS-8.48)

<Alan\_Marcum@NeXT.COM> Tue, 11 Apr 89 14:30:33 PDT

Jerry Saltzer wrote that no old-time pilot would consider taking off without personally verifying the fuel load in the plane, either by looking at it, touching it, or dipping something in it. As a not-so-old-time pilot (though expecting one day to be one), I can say that most of us general aviation pilots (and all of us GA pilots with whom I'll personally fly) STILL verify the fuel load.

Fuel gauges, especially in general aviation aircraft, are NOTORIOUSLY inaccurate. I will not fly a GA plane without having eye-balled or thumbed or dipped the fuel tanks, regardless of rain, high-wing plane with no ladder, or whatever.

Indeed, many airliners fly without this precaution.

"An extraordinary pilot uses his or her extraordinary judgement to avoid having to use his or her extraordinary skills."

- Alan

## ★ Re: More on 1983 Air Canada near-disaster

<Alan\_Marcum@NeXT.COM> Tue, 11 Apr 89 14:34:00 PDT

Henry Spencer wrote that aviations regulations state that the "ultimate authority and responsibility rest with the pilot, nobody else." Whereas this is certainly true in general aviation, this is NOT true in air carrier operations. In air carrier operations, there is a division of labor, where many people other than the pilot in command are responsible for, and have authority as to, various aspects of a flight.

Now, once airborn, it's the pilot's word that goes. Period. However, while on

the ground, during loading and dispatch and such, various ground crew members have authority and responsibility. Of course, it's not THEIR necks on the line in the sky....

- Alan

### ★ Airbus A320 article plus some comments (Leveson, RISKS-8.49)

Greg Rose <greg@softway.oz.au> 11 Apr 89 11:00:46 +1000 (Tue)

>"If a pilot has to make violent changes to the aircraft's attitude
>in an emergency, then the computer will prevent the pilot pushing it
>past design strengths. For example, the computer would prevent the pilot
>putting it into a dive that might break off the tail."

In a past issue of the "Aviation Safety Digest", published (then) by the Bureau of Air Safety Investigation, part of the Australian Department of Name Changes (the Civil Aviation Authority this month) was the following incident report. [From memory]

A single engine light aircraft was flying in heavy cloud and moderate turbulence when it apparently entered a thunderstorm cell. A severe downdraught caused an abrupt descent, followed by wind shear causing a stall, and further descent. The pilot broke free from the base of the cloud, still descending, and saw lots of trees. He pulled back VERY HARD on the controls, recovered control of the aircraft, but felt it was performing strangely, so he landed at the first opportunity.

Subsequent examination of the aircraft showed:

- a) eucalyptus leaves in the undercarriage, presumably from tree skimming.
- b) the wings had undergone permanent deformation, with the tips being now some 30cm higher than normal. The main spar had bent in two places. This was attributed to 'G' forces in excess of the flight envelope of the aircraft.

Now my point: had this been a fly-by-wire aircraft, it would presumably never have been overstressed. The fact that it (and the pilot) would be in little pieces in a rainforest is, however, depressing. The pilot reacted correctly, in that he was "between a rock and a hard place", and chose between certain death due to trees, versus probable death due to airframe failure in flight. He was VERY lucky to come out of this at all, but how would a computer judge between these extremes? (Note that even if the aircraft had had a radar altimeter it would have been hard pressed to tell the height of the treetops. If the flight computer had tried to pull out more gracefully it might still have been an unhappy ending.)

The simple answer is "If it had fly-by-wire, it would have had weather radar, and this would never have happened". True, but to me, irrelevant.

The manufacturers of aircraft build in a healthy safety margin, which in this

case saved a life. But there are at least three choices with a FBW system:

- 1. Allow the computer to fly to the "real" (no safety margin) limit, on the grounds that you can trust it more than a human.
- 2. restrict it to the same performance limitations as you would certify if there was no FBW.
- 3. Forget these safety margins entirely, independent of FBW installations.

I don't like any of the above options. (2) would have killed the pilot above, (1) and (3) are quite similar in end effect, and could see us with a rash of airframe failures due to manufacturing tolerances, corrosion, or miscalculation on the part of the engineers (or their software).

As has been pointed out elsewhere, extreme circumstances do happen, and can sometimes be rectified by humans.

Aside: Harry Harrison, in "Deathworld" written in the mid-sixties, has the hero escape captivity in a spaceship's lifeboat only to crash because the controlling computer won't pull out of a dive quickly enough.

# Re: CDC operating system has passwords in batch files (Stafleu, 8-52)

<LUSOL@VAX1.CC.LEHIGH.EDU> Tue, 11 Apr 89 11:19 EST

I think it is only fair to mention that using SUBMIT\_JOB is just one way of submitting a batch job, and, indeed, NOT the way that our User Services group teaches our users. It took me an hour to find the text that was quoted above, in an older version of a printed manual dated April 1988. In the current version of NOS/VE the JOB/JOBEND construct is what the casual user first sees when reading about batch jobs - this method of submitting batch jobs inherits validation information from the parent job and thus there are no plain text passwords. The primary purpose of SUBMIT\_JOB is to run jobs on OTHER machines.....

Steve Lidie, Lehigh University Computing Center

### NSA and Not Secure Agencies

Curtis Spangler <cas@toad.com> Tue, 11 Apr 89 08:12:04 PDT

San Francisco Chronicle, Chronicle Wire Services, April 11, 1989:

"Computer Group Wary of Security Agency

A public interest group said yesterday that the National Security Agency, the nation's biggest intelligence agency, could exert excessive control over a program to strengthen the security of computer systems throughout the federal government. The group, Computer Professionals for Social Responsibility - based in Palo Alto - urged key members of Congress to focus "particularly close scrutiny" on the agency's role in helping to implement legislation aimed at safeguarding sensitive but unclassified information in federal computers.

"There is a constant risk that the federal agencies, under the guise of enhancing computer security, may find their programs - to the extent that they rely upon computer systems - increasingly under the supervision of the largest and most secretive intelligence organization in the country," it said."

# California's anti-fax-ad bill...

Mark Mandel <Mandel@BCO-MULTICS.HBI.HONEYWELL.COM>
Mon, 10 Apr 89 14:05 EDT

In RISKS 8:52, David M. Gursky wonders about the legality (constitutionality, enforceability) of California's new law against (unsolicited) junk fax, and ends with

- > Of course, this whole message begs the question "How is this a risk
- > to society?"

Junk fax is just as much a menace as junk phone calls that seize the line and won't let go. While junk mail just fills up your mailbox, it doesn't deprive you of legitimate mail unless it piles up to the very top. Junk fax, as long as it's coming in, ties up your machine and makes it impossible for legitimate transmissions to reach you.

-- Mark Mandel



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 8: Issue 55

Wednesday 12 April 1989

# **Contents**

Informing the Public about Risks

Marc Rotenberg

Central Locking Systems

J M Hicks

Social Security Administration Verifying SSNs

**David Gast** 

Not Secure Agencies

**Hugh Miller** 

Re: Cellular Telephones

**Eric Roskos** 

Risk to Sun 386i users

Mike O'Connor via Alan Wexelblat

Infallible Computers and Perry Mason

**Brinton Cooper** 

**Ephraim Vishniac** 

Air Canada and fuel-proof gauges

**Robert Dorsett** 

John Hascall

Info on RISKS (comp.risks)

## Informing the Public about Risks

<mrotenberg@cdp.uucp> Wed, 12 Apr 89 07:57:52 -0700

"Tell the Public the Truth About Risks" (The Washington Post, 4/12/89, p. A22, letter to the editor)

"Jessica Tuchman Mathew's op-ed article `Is There More Risk in the World?' (March 29, 1989) sidesteps one the most basic issues in risk management: the difference between imposed risk and assumed risk. Dr. Mathews states that once people cease to trust 'those who manage and regulate the risks in their lives . . . society's responses become irrational.'

"Public opposition to risky technologies - or technologies whose risks are concealed or lied about by industry and regulators - is not irrational. If they are denied complete and reliable information, people will continue to fight against the introduction of new, unknown risks in their lives.

"Full public information and participation are critical elements in decisions about risk. Unfortunately, in this decade the federal government has consistently restricted public knowledge and involvement in such questions, with decisions often made on the basis of narrowly defined cost-benefit analysis.

"This trend should be reversed. Complete information about various options must reach those upon whom risks will be imposed in order to ensure their involvement in final decisions. For example, in the public debate over meeting future energy needs, nuclear power and its attendant risks should be compared not only with conventional methods of power generation but with increased efficiency and renewable energy sources, federal, state and local government must cooperate and show increasing flexibility in informing, not closing out, the public. The public has a right to know - and to decide."

John E. Young, Research Assistant. Worldwatch Institute, Washington, DC

# Central Locking Systems

J M Hicks <cudat@cu.warwick.ac.uk> Wed, 12 Apr 89 15:29:48 +0100

I expect that the dangers of overlooking the possibility of someone disconnecting the power supply of a security system were hammered out in this forum years ago, but I thought this story was a little different.

A friend of my brother had a car whose alternator broke down. He had the alternator mended. He tried to start the car again. Nothing happened. He realised the battery was still disconnected. He left the car, shut the door, opened the bonnet and reconnected the battery.

Clunk! The Central Locking System locked all the doors of the car, with the keys left in the ignition....

Disconnecting the battery again didn't allow the doors to be opened again --- the manufacturers got that one right.

J. M. Hicks (a.k.a. Hilary),
Computing Services, Warwick University, Coventry, England. CV4 7AL

# Social Security Administration Verifying Social Security Numbers

David Gast <gast@CS.UCLA.EDU> Wed, 12 Apr 89 00:41:33 PDT

The NYT (April 11, 1989) reports that Dorcas R. Hardy, Commisssioner of the

Social Security Administration, told a Congressional committee that the agency had verified millions of SSN's for private credit companies.

The risks of using SSNs and private credit companies have been discussed before. TRW, the nations largest credit reporting company recently proposed paying the SS Administration \$1000000 to have 140 million numbers verified. Risks seem even greater when one company has credit information on 140 individuals--approximately 2/3 of every man, woman, and child in the country.

Phil Gambino, an agency spokesman, reported last month that the agency had verified SSNs only at the request of beneficiaries or employers and had never verified more than 25 numbers at a time. He said such disclosures were required under the Freedom of Information Act.

At the hearing yesterday, Dorcas R Hardy, Commissioner of the SSA, at first denied any other verifications. Later she admitted that in the early 80s, 3,000,000 SSNs were verified for Citi Corp and that last year 151,000 numbers were verified for TRW. Ms Hardy said that the 151,000 numbers were just part of a "test run."

Senator David Pryor, D-Ark, chairman of the Special Committee on Aging, said that previous commissioners, the Congressional Research Service of the Library of Congress, and Donald A. Gonya, chief counsel for Social Security have all decided that such verification is illegal.

David Gast {uunet,ucbvax,rutgers}!{ucla-cs,cs.ucla.edu}!gast

### Not Secure Agencies

Hugh Miller <MILLER@vm.epas.utoronto.ca> Wed, 12 Apr 89 06:19:49 EDT

Re Curtis Spangler's contribution in <u>RISKS 8.54</u> ("NSA and Not Secure Agencies"), quoting the SF Chronicle, quoting the CPSR spokesperson:

- > "There is a constant risk that the federal agencies, under the guise
- > of enhancing computer security, may find their programs to the extent
- > that they rely upon computer systems increasingly under the
- > supervision of the largest and most secretive intelligence organization
- > in the country," [CPSR] said."

I find the "may" most quaint. It strikes me that this is a risk to which we give all too little consideration. In the recent disputes over 'hackers' and the 'ethics' of hacking on this newsgroup I have occasionally noticed some pretty uncritical paeans to security.

The classical philosophers held that knowledge is power. Today we hold that information is power -- not the same thing: worse, in fact.
'Information' in the modern sense is much more structured, hierarchical, and systematic than the classical notion of 'knowledge' allowed. It therefore permits a much greater range and freedom for the employment of our powers and a correspondingly greater degree of control over nature -- human included. As

a result, it aggravates and amplifies the tendency of power to centralise itself to a much greater extent than would have been possible in premodern times. One could, in fact, state a general law of information similar to that of thermodynamics: "The information control (security) of the universe is always increasing." Just as in thermodynamics local excursions in the direction of lesser entropy occur only at the expense of a net gain in entropy for the universe, so in information systems temporary increases in access to information take place at the expense of global increases in control.

Security itself is a (potential) risk -- to those who are not themselves part of the security establishment or who are not in favour therewith. The interests of those who would implement and enforce security measures in information systems must always be balanced against the rights and interests of (1)the users and (2)the subjects, i.e. those about whom the information is being gathered. Remember: just because you are a member of (1) does not mean you are not a member of (2).

Hugh Miller, University of Toronto

## Re: Cellular Telephones

Eric Roskos <roskos@ida.org> Tue, 11 Apr 89 10:22:10 EDT

(Re: Thayer, RISKS-8.53)

- > Has the law changed? I was led to understand that the FCC does not ban
- > the reception of any signal. Of course, banning the reception of
- > certain signals is going to be tough to enforce anyway.

[I originally wrote the following posting in response to the first cellular telephone posting, then decided not to send it because (a) I'd already made several RISKS postings recently and (b) I'm reluctant to comment on legal matters when many legal people seem to get upset by lay-persons doing so. However, in response to the above question I decided to send it in anyway.]

(Re: Den Beste, RISKS-8.52)

- > The article goes on to say that Radio Shack no longer sells that model, and > that the FCC says such eavesdropping is illegal.
- Intentionally listening to cellular communications is a violation of PL 99-508, "The Electronic Communications Privacy Act of 1986," and the violator is subject to a \$500 criminal fine if the interception was of cellular telephone and not for one of the "bad purposes" defined in the legislation (other types of violations have penalties up to \$250,000 for an individual or \$500,000 for an organization). Accidentally encountering such a broadcast while tuning this model of receiver is not a violation if you do not intentionally listen to it, i.e., if you just pass by it in the course of tuning the radio; this issue was specifically addressed in the ECPA.

The cellular telephone frequencies are adjacent to and overlap part of the UHF TV band, so it is also possible to tune them on older, continuous (as vs. discrete)-tuning UHF TV sets. It was reported in the press that the FCC recently stated that it is not illegal to manufacture and sell radios that tune the cellular frequencies, and in the past the FCC has allegedly declined to enforce the ECPA as applied to cellular telephones. On the other hand, the Cellular Telecommunications Industry Association recently used legal measures to force Grove Enterprises, a small dealer of radio equipment in North Carolina, to stop enabling a disabled feature of Radio Shack scanners that allowed reception of cellular telephone. It's interesting to note that Radio Shack was one of the companies listed in the Senate Report 99-541 as "support[ing] the principles involved in the [ECPA] legislation," and they manufacture a radio which has an option jumper that enables reception of these communications. It is currently sold with this option disabled.

There is currently an ongoing debate between radio hobbyists and various sections of the government on application of the ECPA to cellular telephone communications. Recent issues of the monthly periodical \_Monitoring\_Times\_ contain a good bit of editorializing and news items on the subject; there was also a recent book specifically about how to intercept radio telephone communications released by a publisher oriented towards "communications monitoring" topics. It also appears to be the case that a lot of scanners are sold and modified to receive cellular communications, and that the popular opinion is that the ECPA will not be enforced with regard to cellular telephone. From a practical standpoint, this suggests that it is wise to assume that any cellular telephone communications are probably being listened to. From the viewpoint of the potential listener, like the types of unauthorized computer access discussed here recently, in the absence of strong enforcement it is probably largely an ethical consideration: whether or not it is technically legal or illegal, one has to consider whether it is ethical. And, as I've argued in the past, Ethics per se doesn't say whether this sort of activity is "ethical." It's a difficult problem to address, other than simply to realize that the problem exists, and act in an informed manner.

Disclaimers: The above comments result from reading published documents on the ECPA, and are \*not\* the opinions of a legal professional. My interest in the subject is solely in the area of keeping up with security and privacy issues, and does not necessarily reflect the opinion of anyone else.

Eric Roskos (roskos@CS.IDA.ORG or Roskos@DOCKMASTER.ARPA)

## ★ Risk to Sun 386i users (Taken from Sun-nets mailing list)

"Alan Wexelblat" <WEX@dsg.csc.ti.com> Wed, 12 Apr 89 14:55:15 CDT

DISCLAIMER: I merely receive Sun-nets because I am assistant admin here. I have no way to verify the accuracy of this report, but thought it should be distributed. People wanting more information should contact Mike O'Conner directly.

--Alan Wexelblat

----- Forwarded Message

Date: Wed, 12 Apr 89 13:18:49 -0400

From: oconnor@sccgate.scc.com (Mike O'Connor)

Subject: Security hole in 386i login

The login program supplied by Sun for its 386i machines accepts an argument which bypasses authentication. It was apparently added in order to allow the Sun program "logintool" to do the authentication and have login do the housekeeping. This allows any user who discovers the new argument to the login program to become root a couple of ways.

[...]

Mike O'Connor oconnor@sccgate.scc.com 301-840-4952 | 703-359-0172

ps: Mike Rigsby (rigsby@ctc.contel.com) tells me that at a 386i SOS administration class he attended, he was informed that this access path was a design feature put in for forgetful administrators but that the class was told to keep it a secret. I find this surprising, if true, since this is the OS that Sun claims "meets the spirit of C2 specifications." Then again, maybe I understand even less of the C2 specs than I thought I did.

----- End of Forwarded Message

# ✓ Infallible Computers and Perry Mason (Dave Curry, RISKS-8.54)

Brinton Cooper <abc@BRL.MIL> Wed, 12 Apr 89 17:19:05 EDT

>If I were the guy on the stand, I would have denied it all and forced Mason to >prove that the time of day clock on the computer was correct at the time I >last edited that file.

Actually, in the experience of the "average viewer" of a Perry Mason show, this is probably a valid representation. If they know computers at all, they're probably PC-class things containing a clock card. Just a little diligence sets things up OK; most folks probably like the idea of a date/time stamp on documents that they're constantly revising.

So, while it wouldn't have happened in many of our labs, it's probably reasonable to have skipped Mason's providing "proof" that the clock was correct since it's entirely reasonable, in this kind of case, that it probably was.

Brint

### Infallible computers :-)

<ephraim@Think.COM>

Wed, 12 Apr 89 16:29:29 EDT

In RISKS 8.54, davy@riacs.edu reports on Perry Mason's latest:

"Anyway, the show demonstrates the fallacy of assuming that since the information came from a computer, it is somehow ennobled,..."

But it didn't come from just any computer, it came from a Macintosh!

Seriously, I've come across several Macs here at TMC with clocks about four hours slow. Why? They were manufactured and tested on Pacific Standard Time, and here it is Eastern Daylight Time. Contrariwise, I've seen and heard about many Macs with clocks that run fast by several minutes per month. Clock accuracy requires maintenance!

Ephraim Vishniac

## ✓ Air Canada and fuel-proof gauges (Wales, RISKS-8.51)

Robert Dorsett <mentat@dewey.cc.utexas.edu> Tue, 11 Apr 89 20:27:16 CDT

I have been trying to get more information on how the 767's systems work, but I think I should clarify something here. People seem to be getting the idea that the romantic notion of sticking a dipstick in a fuel tank is a practical, easy accomplished act in an airliner. It isn't.

Putting aside the fact that one has to get on the wing (and add structural and maintenance support for the traffic areas), on Boeing aircraft, at least, the overwing fuelling ports are fastened with several dozen screws. It is a pain taking the ports off and putting them back on. A lengthy, expensive process. Normally, fuelling is done on the starboard wing, through an underwing high-pressure nozzle.

To give an idea of how unattractive overwing fuelling is, recently, an Aeromexico 727 diverted to an ex-WWII bomber base in Galveston, TX, during a thunderstorm. They were short on fuel. Galveston has a full-service FBO, and routinely caters to executive jets--but they didn't have the right nozzle size. Instead of opening the overwing hatches, they sent a car off to Houston to fetch the right adapter, sixty miles away--a total delay of about four hours.

All of this rather makes me doubt the "dipstick" story on the Air Canada 767, unless there's a new, specialized system that avoids the filler port. Or, more likely, "dipstick" is slang for a secondary automated system.

In the old days (on props), "inspections" WERE used, but often required custom-designed dipsticks. A few planes were lost because the wrong dipstick was used (improper graduations).

In practical airliner work, fuel is calculated using four methods:

- 1. The amount pumped in (by weight, on the truck);
- 2. Gauges near the wing (totalizers);

- 3. Individual tank quantity gauges and a totalizer gauge in the cockpit (merely knowing how much fuel is left is not adequate; one must know WHERE it is, due to loading considerations).
- 4. The amount burned (the fuel passed through the engines, fuel flow).

Fuel management is a continual cross-check of all these factors (that's what the flight engineer, if present, is there for). Occasionally, things screw up (as in the case of the UA 747 near Japan, which "ran out of fuel," but was found to have 30,000 lbs left in the center tank--they actually lost three engines). Overfilling is also more common than it should be--if you ever see a plane dripping liquid, it's probably an overfilled tank. The fire trucks won't be far behind...

>Henry Spencer wrote that aviations regulations state that the "ultimate >authority and responsibility rest with the pilot, nobody else." Whereas this >is certainly true in general aviation, this is NOT true in air carrier >operations. In air carrier operations, there is a division of labor, where >many people other than the pilot in command are responsible for, and have >authority as to, various aspects of a flight.

Legally, they have no authority. Under FAR 91.3, the pilot in command is directly responsible for, and is the ultimate authority as to, the proper operation of the aircraft. In PRACTICAL work, as other posters have noticed, other people assume a de facto responsibility. However, once the captain signs the dispatch papers, he is LEGALLY responsible. If the captain signs off with an improperly loaded aircraft, or with dry fuel tanks, it is HIS legal responsibility.

The "ground crew" concept came into being during the 60's, and was a result of human-resource studies. It usually works, but ground people do make mistakes. The pragmatic pilot will always double-check the figures and, at least, make an effort to determine whether the figures (and the general status of the airplane) are in the ballpark. We are starting to see a return to a more "hands on" management style.

Robert Dorsett

### ★ Air Canada and fuel-proof gauges (Wales, RISKS-8.51)

John Hascall <a href="mailto:hascall@atanasoff.cs.iastate.edu">hascall@atanasoff.cs.iastate.edu</a> Tue, 11 Apr 89 20:18:44 CDT

Commercial aircraft rarely take off with a full fuel tank, there is no profit to be made in lifting a bunch of extra fuel. Only enough to make it to the primary destination and secondary landing site plus some extra for holding is loaded. Any extra would just have to be dumped anyway to meet the safe landing weight.

So eyeballing the tank to see if it was full would be useless, you would need to use the dipstick.

John Hascall

[The next step is a computer program that checks the fuel levels, the flight destination, the weather data, and the plane load (among other things) and determines whether there is enough fuel. If pilots came to trust THAT computer program -- and the sensors, computer data. etc. -- then my eyeballs would be rolling. So, let's hear it for intelligent people, whether or not they use dipsticks! 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 8: Issue 56

Thursday 13 April 1989

## Contents

Student grants debited instead of credited

John Harper

Electronic Truant Officers

Mike McNally

"Virus" arrest in New Jersey

A. Michael Berman

H.D. Thoreau on Risks of Believing Computations

**David A Honig** 

Knowledge and Power

David Guaspari

"Malicious" computers?

**Clifford Johnson** 

Re: Infallible Computers and Mason

Jack Holleran

HP MPE V/E Batch Security

**Brown** 

More on the Sun 386i security hole

David C. Kovar via Alan Wexelblat

Info on RISKS (comp.risks)

### Student grants debited instead of credited

John Harper <HARPER@rs1.vuw.ac.nz> Thu, 13 Apr 89 16:58:30 NZT

Student grants in New Zealand are now paid by direct credit from the university's bank account to the student's. On Tuesday Victoria University sent a tape with the details to its bank, the Bank of NZ, which passed it on to Databank, the NZ banks' centralised computer centre. One (human) error meant the university was apparently asking for debits of a total of about \$2,000,000 from some 4700 students instead of credits to their accounts. Databank did this although of course the university was not authorised to debit the students. According to today's "Dominion" newspaper BNZ may have spotted the error. On Wednesday a certain amount of chaos ensued, with students' banks

saying all their cheques would be honoured that day and no overdraft fees applied. Corrections were made that night. It seems that Databank had no senior staff on duty on Tuesday night when the wrong transactions occurred, and guessed wrong on finding conflict between BNZ and Victoria University of Wellington instructions.

John Harper, Mathematics Department, Victoria University, Wellington, NZ

#### Electronic Truant Officers

Mike McNally <m5@lynx.uucp> Thu, 13 Apr 89 11:18:43 PDT

During a recent episode of the PBS series "Learning in America", the cameras were taken through a trade show at which computer and software vendors pitched high-tech teaching aids to school board purchasing agents. Aside from possible (and clearly debatable) RISKs to the brains of American schoolchildren (my child was taught by a computer; she must always be right!), a more ominous idea was presented. A company whose name I cannot recall was demonstrating a software system to track attendance. It included a feature whereby parents would be automatically notified (by mail, I suppose) of their childrens' absences:

"Where were you last week?!?"

"In school, mom!"

"Wrongo! The school computer says you were absent 12 days last week!" (\*\*whack\*\*)

Mike McNally, Lynx Real-Time Systems

[Incorporeal banishment leads to corporal punishment! PGN]

## "Virus" arrest in New Jersey

A. Michael Berman <berman@pilot.njin.net>
Thu, 13 Apr 89 10:03:47 EDT

From the Phila. Inquirer, April 12, 1989. Page One, New Jersey/Metro section.

"Ex-worker charged in virus case -- Databases were alleged target", by Jane M. Von Bergen, Inquirer Staff Writer

A former employee was charged yesterday with infecting his company's computer database in what is believed to be the first computer-virus arrest in the Philadelphia area.

"We believe he was doing this as an act of revenge," said Camden County Assistant Prosecutor Norman Muhlbaier said [sic] yesterday, commenting on a motive for the employee who allegedly installed a program to erase databases at his former company, Datacomp Corp. in Voorhees [N.J.].

Chris Young, 21, of the 2000 block of Liberty Street, Trenton, was charged in Camden County with one count of computer theft by altering a database. Superior Court Judge E. Stevenson Fluharty released Young on his promise to pay \$10,000 if he failed to appear in court. If convicted, Young faces a 10-year prison term and a \$100,000 fine. Young could not be reached for comment.

"No damage was done," Muhlbaier said, because the company discovered the virus before it could cause harm. Had the virus gone into effect, it could have damaged databases worth several hundred thousand dollars, Muhlbaier said.

Datacomp Corp., in the Echelon Mall, is involved in telephone marketing. The company, which has between 30 and 35 employees, had a contract with a major telephone company to verify the contents of its white pages and try to sell bold-faced or other special listings in the white pages, a Datacomp company spokeswoman said. The database Young is accused of trying to destroy is the list of names from the phone company, she [sic] said.

Muhlbaier said that the day Young resigned from the company, Oct. 7, he used fictitious passwords to obtain entry into the company computer, programming the virus to begin its destruction Dec. 7 --- Pearl Harbor Day. Young, who had worked for the company on and off for two years --- most recently as a supervisor --- was disgruntled because he had received some unfavorable job-performance reviews, the prosecutor said.

Eventually, operators at the company picked up glitches in the computer system. A programmer, called in to straighten out the mess, noticed that the program had been altered and discovered the data-destroying virus, Muhlbaier said. "What Mr. Young did not know was that the computer system has a lot of security features so they could track it back to a particular date, time and terminal," Muhlbaier said. "We were able to ... prove that he was at that terminal." Young's virus, Muhlbaier said, is the type known as a "time bomb" because it is programmed to go off at a specific time. In this case, the database would have been sickened the first time someone switched on a computer Dec. 7, he said

[note -- it makes me kind of sick to see the term "sickened" applied to a database... sigh]

Norma Kraus, a vice president of Datacomp's parent company, Volt Information Sciences Inc, said yesterday that the company's potential loss included not only the databases, but also the time it took to find and cure the virus. "All the work has to stop," causing delivery backups on contracts, she said. "We're just fortunate that we have employees who can determine what's wrong and then have the interest to do something. In this case, the employee didn't stop at fixing the system, but continued on to determine what the problem was." [hear, hear!]

The Volt company, based in New York, does \$500 million worth of business a year with such services as telephone marketing, data processing and technical support. It also arranges temporary workers, particularly in the data-processing field, and installs telecommunication services, Kraus said.

[As usual, everything is now a 'virus', even a nonreplicating timebomb. PGN]

#### ★ H.D. Thoreau on Risks of Believing Computations

David A Honig <honig@BONNIE.ICS.UCI.EDU> Thu, 13 Apr 89 17:28:16 -0700

From Walden, Ch. 1 "Economy":

..to keep yourself informed of the state of the markets, prospects of war and peace every where, and anticipate the tendencies of trade and civilization, ---taking advantage of the results of all exploring expeditions, using new passages and all improvements in navigation; ---charts to be studied, the position of reefs and new lights and buoys to be ascertained, and ever, and ever, the logarithmic tables to be corrected, for by error of some calculator the vessel often splits upon a rock that should have reached a friendly pier...

#### Knowledge and Power

<oravax!nestor.UUCP!davidg@wrath.cs.cornell.edu>
Thu, 13 Apr 89 15:26:23 EDT

Corrections to some semi-philosophical remarks in a recent posting: Hugh Miller, Not Secure Agencies, in <u>RISKS-8.55</u>:

> The classical philosophers held that knowledge is power.

If we give "classical" its usual meaning, no such philosopher "held that power is knowledge" (or, at any rate, none known to me). The famous aphorism comes from Bacon, and what he was doing was proposing a radically new definition: that nothing counts as true knowledge unless it enables us to intervene in and control the material world. All the rest was mumbo-jumbo. This was part of an explicit attack on (more or less) everybody who preceded him, especially the Schoolmen.

Note: There's a meta-problem with phrases like "the classical philosophers [believed this or that]" -- for the simple reason that there were many different ones, and they often disagreed.

> 'Information' in the modern sense is much more structured ... than the classical notion of 'knowledge' allowed.

Comparing information and knowledge is like asking whether the fatness of a pig is more or less green than the designated hitter rule. Let's take Plato and Aristotle as exemplars of "classical" views on "knowledge." For both of them, knowledge concerns the highest truths about the cosmos and mankind's place in it, and is aspired to by the very best kind of human being. Such cannot be said of lists of social security numbers.

David Guaspari

### ✓ "Malicious" computers?

"Clifford Johnson" <GA.CJJ@Forsythe.Stanford.EDU> Thu, 13 Apr 89 16:45:19 PDT

From: ficc!peter@uunet.UU.NET

- > One thing to bear in mind is that the computer can be mistaken, but
- > it can't be malicious. The computer program won't deliberately try to defraud

Hmmm. Depends on your definition of "malicious." A large bank I worked for was found in court to have programmed its computers so as to systematically defraud its customers of their full compound interest. Whether the program into which the fraud was built was "malicious" is largely a matter of terminology.

Let me turn the issue around somewhat - can a computer recognize "malice" in a person? Believe it or not, some computerized psychological tests (that are regularly admissible in court as evidence) purport to be able to diagnose malicious tendencies. I was once compelled by a court to submit to such an examination, despite my academic protest that such tests were scientifically invalid (which was established statistically in the 1960s).

The computer reported that I didn't have a sense of humor, which I still find amusing. However, the widespread use of such tests is definitely not amusing.

## ★ Re: Infallible Computers and Mason (RISKS-8.54)

Jack Holleran <Holleran@DOCKMASTER.NCSC.MIL> Thu, 13 Apr 89 10:06 EDT

In reference to Dave Curry's response about the guy on the stand. Mason doesn't have to prove he was guilty of the crime; he has to prove that his client is not guilty. Ergo, it wouldn't matter if the guy on the stand denied everything and forced Mason to prove anything. The bottom line is Mason by discussing the "directory" could introduce some doubt to the District Attorney's argument. Normally, if the case is not provable "beyond a reasonable doubt", a verdict of "not guilty" is usually given.

Of course, since Mason always does such a good job, the DA doesn't have to work hard for the next trial. But then again, Mason might defend the "guilty" guy successfully since "was the directory acquisition legal"?

So much for supporting Mason writers...

I agree strongly with Dave's arguments since many people do accept computer printouts as infallible facts and gospel. I wonder how many RISK debates are accepted because they appear in the RISK forum... I also wonder how many people use the RISKS forum discussions/debates to support local opinions... The computer word/document/listing has become a very powerful tool (just like statistics) and many people use it to their advantage.

Jack Holleran (This is strictly an opinion not based on anything legal.)

### **HP MPE V/E Batch Security**

<brown@aerospace.aero.org>
Thu, 13 Apr 89 08:43:46 -0700

I'd like to respond to a posting by Brian McMahon, Administrative Computing, University of Maryland in which he states: "May I add to the list of flagrant security violators the Hewlett Packard Corporation? Under MPE/V (the current OS for HP/3000 machines), all batch jobs must begin with a JOB card (those of you living in the late 1980s, substitute "line of text") which contains user and group passwords in plain text.

"Interestingly, one of our systems programmers (who shall remain nameless) spoke of this as a FEATURE, because it allows users to submit batch jobs for other accounts!"

The C2 evaluated version of MPE V/E, which was announced in October of 1988, allows the security administrator to configure the system to remove this vulnerability. In particular, to quote from the Final Evaluation Report:

"Prevention of password exposure in batch submissions is effected by rejecting embedded passwords in job cards, prohibiting cross streaming [mentioned in the second paragraph above], and allowing System Manager and Account Manager to stream subordinate's jobs, and a user to stream one's own jobs, without having to supply passwords. A privileged interface, STREAMJOB, is provided which allows privileged mode programs to start jobs without having to supply passwords."

Obviously, word hasn't gotten out to everyone about how the C2 secure version of MPE V/E works, but I know it does since I was team leader of the National Computer Security Center evaluation team. It is true that a customer must pay extra to get the Security Configurator software which will turn on the above features, but the ability to prevent job STREAMing with exposed passwords is there in all versions of release G.03.04 and later. You have to have the Security Configurator to configure it that way; otherwise it will default to the previous way of handling STREAMing, which requires embedded passwords. This is known as backward compatibility, and HP is hardly the first company to worry about that.

### ✓ More on the Sun 386i security hole

"Alan Wexelblat" <WEX@dsg.csc.ti.com> Wed, 12 Apr 89 16:59:41 CDT

Taken from Sun-nets again:

Date: Wed, 12 Apr 89 15:48:28 -0400

From: -David C. Kovar <daedalus!corwin@talcott.harvard.edu>

Subject: Re: Security hole in 386i login

Reply-To: daedalus!kovar%husc4@talcott.harvard.edu

Several phone calls to Sun later ... Someone at Sun claims that it is a

"known security hole in 4.0.1 and will be patched in the next release due out at the end of May." I pointed out that it was more like a known security trapdoor feature and there wasn't much argument on the point. [...]

-David C. Kovar

Technical Consultant ARPA: kovar@husc4.harvard.edu

Office of Information Technology BITNET: corwin@harvarda.bitnet

Harvard University Ma Bell: 617-495-5947



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 8: Issue 57

Saturday 15 April 1989

#### Contents

H.D. Thoreau on Risks of Believing Computations

Jim Haynes

Airbus 320

**Brian Randell** 

1,000 Pilots Face ban

**Dermot Williams** 

RFI and elevators

Robert A. Morris

Electronic Truant Officers

Carolyn M. Kotlas

Michael R. Hoffman

**Ed Robertson** 

Re: Computer CAN attempt to defraud you

**Hugh Davies** 

Computer maliciousness

Peter da Silva

Info on RISKS (comp.risks)

#### H.D. Thoreau on Risks of Believing Computations (RISKS-8.56)

Jim Haynes <haynes@ucscc.UCSC.EDU> Thu, 13 Apr 89 22:08:56 -0700

This reminded me of an anecdote in one of the early books about computers, which was used to illustrate Babbage's insistence that the Difference Engine should produce as output plates for printing the results, lest someone's error in copying/typesetting introduce an error. (Might have been the book "Faster, Faster" by W. J. Eckert.)

There was a brief period in which England and Spain were on good terms with each other. An English admiral invited a Spanish admiral aboard his flagship for a visit, during which he presented the visitor with a beautifully bound copy of the English navigational tables. After the visit the Spanish fleet sailed away and was never heard from again. It seems the English never used their own navigational tables, knowing them to be full of errors; they always used the French tables.

[Turn the tables on the fleet afoot? PGN]

#### Airbus 320

Brian Randell <Brian.Randell@newcastle.ac.uk> Fri, 14 Apr 89 18:28:29 BST

I recently obtained - from Bev Littlewood - a copy of an article in France-Soir for 18 February about computer-related problems of the Airbus 320. In case it can, despite the passage of time, still add usefully to the information that has been made available in the Anglo-Saxon (French for UK plus US!) press, I am providing an almost complete translation, in which I have endeavoured to retain the flavour and style of the original article. (My apologies for the amateur nature of the translation and of the inadequacy of the dictionary that I had available to me at the time!)

Brian Randell, Computing Laboratory, University of Newcastle upon Tyne

AIRBUS 320: THE COMPUTER REFUSES TO PASS ON THE PILOT'S INSTRUCTIONS: One of the Incidents which has caused Aerospatiale to return the machines to "marbre" [?]

Less than one year after it first went into service, the Airbus A320, the most sophisticated civil airliner existing, has to go back to the "marbre" [?]. A simple revision after thousands of hours in the air? Not just that!

After going into service in April last, the plane is "chouchoute""[?] by its builder, Airbus-Industrie, and the air lines. All the improvements capable of being made to the latest Airbus are made under the control of DGAC (Direction Ge'ne'rale de l'Aviation Civile). "The A320, like all new machines, is in its period of debugging ["de'verminage"]," emphasized Daniel Tenebaum, the boss of DGAC. "It is above all a question of removing faults which have appeared since it first went into service."

#### STRAIGHT AT A MOUNTAIN:

During critical phases - landing and take-off - the computer system shows only the most dangerous alarms. "This is a wretched problem", explained an Air France captain, "Certain failures are recorded by the computer, but the pilots are informed only later".

Paul Baud, the flight trials director of Airbus-Industrie explains: "To ease the task of the pilot, only the problems which relate directly to critical phases are communicated to him: fire in the engines, the baggage hold, or in the toilets."

But there are worse ones. The computer system (nicknamed the "Little Genius") sometimes escapes from the control of the crew. "I am going to land at Geneva in my A320, and it happens that the altitude indicators show `hauteurs farfelues' [incorrect heights?]. Luckily the airport urgently advised me of

this. Otherwise we would have flown straight into the mountain!" Immediately, the captain demanded that the computer be replaced as being not completely reliable.

Worse. The case of the pilot who saw with horror his computer indicating "full fuel load" when he started his descent to the airport in West Berlin. And the famous "Little Genius" refused to let him take over manual control. "We very nearly had a catastrophe", said the pilot.

The cause, it seems, is the electrical power supply. "We have screened[?] all electrical resistances" ["Nous avons passe' au crible l'ensemble des re'sistances"], insists Paul Baud. "There was though a failure. Henceforth, the on-board computers will be fitted with higher performance diodes."

#### A FAULTY COMPUTER:

They will even improve the transformers-rectifiers. These serve to supply the A320's automation systems, in modifying the the alternating and the direct current. Nevertheless, Airbus-Industrie points out that all the flight-critical mechanisms are duplicated. One defective computer is thus immediately replaced by its twin.

[Paragraphs about complaints regarding noise-levels in the A320, and plans regarding improved sound-proofing.]

## ✓ 1,000 Pilots Face ban

Dermot Williams <DWILLH89@IRLEARN.BITNET> Fri, 14 Apr 89 19:01:33 GMT

From Dublin's EVENING HERALD of Thursday 13th April, without permission:

"1,000 Pilots Face Ban"

The US Federal Aviation Administration said it planned to suspend or revoke the licences of more than 1,000 pilots who lied about past alcohol or drugs convictions.

The FAA said about 10 per cent of them were commercial airline pilots and the rest were private pilots.

The FAA said it got the names of more than 6,000 pilots through a computer match of medical applications, criminal records and state motor vehicle records.

Any of the pilots on the list care to comment? Do you feel that this is a fair or foul use of computer databases?

Dermot Williams, University College Dublin, Dept. of Computer Science

[In an effort to make sure we stick to the computer risks, and not compete with the aviation BBoards on technical nuances, I suggest that some of the

pending submissions to RISKS might better be redirected elsewhere. This item is clearly a computer database problem, not an aviation problem. PGN]

#### RFI and elevators

Robert Morris <ram@typo.UUCP> Thu, 13 Apr 89 22:09:59 EDT

Dave Horsfal writes in Risks 8.54:

I have a little hand-held (amateur) transceiver, generating just 3 watts on 147 MHz from a "rubber duck" antenna - very inefficient. When I'm in the mood, I trigger it next to various bits of electronic equipment, just to test their RF susceptibility. ...

This is distressing behavior from a licensed amateur radio operator. In the US, this might subject one to revocation of the license and possibly criminal penalties if the action caused damage or injury. In the US, amatuer radio transmissions are restricted in purpose, and testing RFI rejection of commercial equipment is not one of them. Even if the manufacturer were wholly negligent in their RFI rejection, the amatuer "investigator" of this fact could reasonably be expected to understand the consequences of probing this inadequate security. For example, I rather doubt that any one would make such an investigation of, say, someone's pacemaker. In my opinion, amatuer radio operators have approximately the same responsibility as did the author of the Internet worm. They have substantial technical knowledge and good reason to believe that their action could cause malfunction, and in this case, possible injury.

Robert A. Morris KA1BWN

[Robert Morris was a signer of the Declaration of Independence. We have now had at least FOUR different namesakes contributing to or discussed in RISKS. I hope no one is confused. PGN]

### Electronic Truant Officers (Re: RISKS-8.56)

Carolyn M. Kotlas <kotlas@uncecs.edu> 14 Apr 89 12:40:53 GMT

My daughter's high school (and several others in this area) has had such a notification system in place for several years. I don't know how much a part the school's computers play in this, but the notification is in the form of a telephone call to the home and a generic recording that is played. Something along the lines of "Your child was reported absent in one or more of his/her classes today." The source of problems (or "risks") of this system is human, not computer-based. Every time I received the recording, my daughter's absence was excused, usually because of a school field trip that had been approved by the school; so if there's poor coordination between teachers and administration, parents will receive false alarms. (Which, like too many cries of "Wolf!" may lessen a parent's belief in any real reports of absences.)

Also, since the calls are usually generated at a predictable time in the evening of the absence, truants could just take the call for the parent and

report it as a wrong number. (I've also heard of people without children getting these calls, either due to typos in the student's records or misdialing of the number.) So much for an infallible reporting system here.

-- Carolyn Kotlas, UNC-ECS, Research Triangle Park, NC

#### Re: Electronic Truant Officers

Michael R. Hoffman <h44394@leah.Albany.EDU> Fri, 14 Apr 89 13:13:43 EDT

When I was in my Sophomore year at The Bronx High School of Science, they implemented a computerized attendence scheme. Every student was given a number (welcome to the real world... forget your name, you are now ####) which was used to trace the student through their years at school. When attendence was taken in classes and in Homeroom, the teachers would fill out "bubble" sheets which were passed through a scanner to the central computer, which was located somewhere in Manhatten!

They quickly found many problems in the system. Errors in filling in the wrong bubbles, the computer crashing, students forgetting their number, and students who would cut Homeroom (which meant "Absent for Day") yet were not marked absent in certain classes, really screwed the school administration up.

And, as with most other computer systems, there were ways around the system. Supposedly being the "brightest students in the country" (YEAH, Right!! :-}), you can imagine the fun we had beating it.

In a word, computerized school attendence systems are a JOKE! And they don't help with convincing the students that are REAL people, not just cogs in the system.

#### Electronic Truant Officers (Re: RISKS-8.56)

Ed Robertson <edrbtsn@iuvax.cs.indiana.edu>
14 Apr 89 23:00:24 GMT

One evening last week the phone rang and I answered to hear a sepulcral electronic voice announce that my son, whom I know was in school, had been absent from all of his classes that week.

The best part of this system, from the schools point of view, is that there's not even any chance to question that electronic voice.

Edward Robertson, Computer Science Dept, Indiana U., Bloomington, IN 47405-4101

#### Re: Computer CAN attempt to defraud you

<"hugh\_davies.WGC1RX"@Xerox.COM> 14 Apr 89

linden@Sun.COM (Peter van der Linden) asserts that a computer can defraud

you. His story about the pie factory is seriously flawed.

- 1) The computer is just a tool. You are being defrauded by the management of the pie factory, in the same way you are defrauded by the taxi driver who short changes you rather than by his taximeter.
- 2) Weights and measures are controlled by legislation. It may be immoral to take advantage of the loopholes in that legislation, but it is not dishonest. If the law is unsatisfactory, get it changed.
- 3) In the pie factory case, before automation, 50% of consumers of a 4oz. pie were getting \*more\* than they had paid for. I wonder how many of them wrote to the factory to offer more money?
- 4) Computer weighing systems do \*not\* allow "an accuracy hitherto unobtainable". (I wrote potato chip weighing systems for two years for a living). What they generally do is allow repeatability in weighing, i.e., a narrowing of the distribution curve of the weights dispensed, which then allows a slight reduction in the 'set-weight', at an enormous saving to the producer, spread over millions of items, but a minimal impact on the consumer of a single item.
- 5) Peter says "if the pie was a "4oz" pie, the bakers were permitted to range from 3.5 to 4.5oz". This sounds unlikely to me. I am not familiar with American weights and measures legislation, but the law is usually either formulated such that \*no\* pie may weight less than 4oz which means that the average pie must actually weigh 4oz plus twice the standard deviation of pie weight (at least depends on how assiduous you want to be in avoiding prosecution!), or there is some kind of limit on what proportion of pies may weigh less than the marked weight. If the control is merely on the average weight, given two pies, I'll have the 8oz pie and you can have the empty carton! In either case, it is in the manufacturers interest to reduce the standard deviation as much as possible, which is what the computer allows. In fact, the real problem is not weighing the pies, or whatever, but accurately dispensing the filling. In the EEC, all products are divided into two categories, 'easy to pack', and 'difficult to pack' with the former having tighter controls than the latter.

When I was weighing potato chips, one of the things we did was make sure each and every packet had at least the legal minimum content. This goes part-way towards ensuring that every consumer gets what he paid for.

**Hugh Davies** 

## ✓ Computer maliciousness (Re: RISKS-8.56)

<ficc!peter@uunet.UU.NET>
Fri, 14 Apr 89 13:38:50 -0400

Having been roundly chastened for claiming that a computer can not be malicious, let me explain this point more fully. A bank may have policies that are malicious, and may embody these policies in a computer program. I would not deny that... the point I'm making, though, is that the computer software can be assumed to embody the policies of the bank. Subject to bugs and design

flaws, of course, but it's the bank's policies.

An agent of the bank, then, has a reason to stand by the computer:

While the software may have bugs, they can be reasonably certain it is not intended to defraud the bank. So long as the bank has reasonable policies, they can also assume that there's nothing in the program intended to deliberately defraud its customers. They have no such certainty about the customers themselves.

The problem comes when a customer has documentation to substantiate his or her claim, or they know there's a bug, and they still don't act.

Peter da Silva, Xenix Support, Ferranti International Controls Corporation.



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 8: Issue 58

Monday 17 April 1989

## **Contents**

Cruise Missiles with "Polish"

Ralph Vartabedian via Nancy Leveson

Computerized parts supply

<u>Jim Haynes</u>

RFI and Elevators

**Martin Ewing** 

Aegis the almighty

**Henry Spencer** 

Thoreau and Navigation

**Eric Roskos** 

Risks of automatic order entry in restaurants

**Daniel Klein** 

Re: Most Accurate Clock

Clay Jackson

Fuel Management/Mis-management

Mike Brown

Companies mask ANI to calm callers

**Bob Wallace via GEBM** 

The dangers of electric windows

Martin Cooper

Careless tape transfer procedures

**Peter Jones** 

Info on RISKS (comp.risks)

#### Cruise Missiles with "Polish"

Nancy Leveson <nancy@commerce.ICS.UCI.EDU> Sat, 15 Apr 89 13:41:29 -0700

From the L.A. Times, Saturday, April 15, front page.

HOW CONCERNED WORKERS BLEW WHISTLE AT NORTHROP by Ralph Vartabedian, Times Staff Writer

On her very first day at Northrop's Western Services Department in El Monte, which produced guidance devices for nuclear-armed cruise missiles, Florence Castaneda said she knew that "something was terribly wrong." In an electronics "clean room," Northrop employees were smoking cigarettes, boiling water for soup, eating lunch at their work stations and watching soap operas on a television set mounted on the supervisor's desk, she recalled. Castaneda noticed that instead of using industrial solvents to clear and prepare circuit boards for soldering, workers were using a jar of Tarn-X, a retail brand of polish for silverware. "There was a price tag on it from Thrifty Drug Store," she recalled. "I hadn't seen this kind of work being done in the aerospace industry." ...

As a result of their efforts, a federal indictment was filed earlier this week, charging their formal supervisor, Charles Gonsalves, with criminal fraud.

Tests were allegedly faked and in some cases not performed at all on cruise missile guidance systems and on stabilization systems for Marine Corps jet fighters, the indictment said. Besides Gonsalves, criminal charges were filed against Northrop itself, two high-ranking executives and two other supervisors. Northrop has said the criminal changes against it and two current executives are "unwarranted," but the firm has acknowledged that problems existed at the plant and that Gonsalves and three other employees have been fired. ... Not only was the plant manager, Gonsalves, charged with fraud, but the factory's quality assurance supervisor and its chief engineer were indicted.

Unlike many other defense industry whistle-blowers, Castaneda has no financial stake in any False Claims Act law suits, which individuals can bring on behalf of the government and share in the damages. She was motivated by a sense of concern over "those nuclear missiles out there" that she always worried "could be the start of World War II." ... "I called the FBI in November, 1986. They told me I sounded like a disgruntled employee and that it was a case of sour grapes," Castaneda recalled. (Justice Department officials declined to comment on Castaneda.) It was not until a nephew in the Air National Guard arranged a meeting with Air Force agents from the Office of Special Investigations that anybody would listen to her story.

In January, 1987, an OSI agent [met with Castaneda and fellow workers Barajas and Meyer]. "Florence had earlier attempted to contact Northrop, but nothing ever happened," Barajas said. "Pat Meyer and Florence called back east to Precision Products Divison [the corporate parent of Western Services Department' to say problems were going on. After that, absolutely nothing was done. It disgusted everybody. We knew that if we tried to complain, nothing would be done." Barajas said that he wrote an anonymous letter to corporate executives at Northrop, but the letter eventually ended up back with Gonsalves. "He posted it on the bulletin board to tell everybody that it wouldn't do any good to complain. He laughed at it. He said, "Whatever fool tried it, it didn't get anywhere."

After the investigation was launched in 1987, however, government agents met with the employees once every other week at Barajas' house. Barajas provided investigators with a computer tape used to falsify tests on cruise missile systems built at the plant.

[The rest of the article describes details of the investigation including wiring one of the employees with a tape recorder. There is also a bizarre

story about a psychologist who had been assigned to Castaneda after a temporary disability claim in April 1985, who visited Castaneda at home three times a week for two hours each time for several months. "She told me to forgive Northrop and to forgive Mr. Gonsalves -- to ask God to forgive them -- and to just go back to work," she said.]

## Computerized parts supply

Jim Haynes <haynes@ucscc.UCSC.EDU> Mon, 17 Apr 89 13:41:49 -0700

From a book review in Science magazine, 7 Apr 89

"He even tells us about his disappointment upon learning that a part he was ordering from a catalogue couldn't be shipped until the next week, in spite of a promise in the catalogue of same-day service.

'You must have a very old catalogue,' he was told, without a trace of irony. 'Now we have a computer.'"

The book reviewed is "Ideas and Information: Managing in a High-Tech World" by Arno Penzias; Norton, New York, 1989. 224 pp. \$17.95

### ✓ RFI and Elevators (Morris, RISKS-8.57)

Martin Ewing <mse%b2red.caltech.edu@lago.Caltech.Edu> Sun, 16 Apr 89 23:30:05 PDT

[On the subject of radio amateurs transmitting in elevators:]

In fact, radio amateurs are allowed to do various things other than talk to each other. They may operate radio control aircraft, they may evaluate antennas, and they may run RFI tests -- usually to minimize interference from their own transmissions to TVs, etc. Horsfal's downfall [oops, no pun] might come if he did not properly identify himself with his call sign.

The more interesting point for RISKS is that a 3-watt handitalkie is NOT an especially unusual device to be found on an elevator. Our buildings & grounds people carry them around all the time, and they certainly aren't shy about using them near elevators -- or your pacemaker, for that matter.

Elevators and other 'smart' safety-critical gadgets like automotive microcomputers must have a defined behavior in any likely electromagnetic environment. They don't have to work, but they should fail safe.

Martin Ewing, AA6E, Caltech Radio Astronomy

### Aegis the almighty

<henry@utzoo.UUCP>

Sun, 16 Apr 89 23:16:29 -0400

In the Feb 27 Aviation Week, in an article on US Navy antisubmarine warfare and future plans for same:

The fundamental problem with ASW is that it is very complicated. There is no single system that is a panacea, like Aegis is to air defense, Rear Adm. James R. Fitzgerald, director of the antisubmarine warfare division of naval warfare for the chief of naval operations, said. "If there were, the Navy would buy a lot of them and declare the problem solved."

The view of Aegis that is revealed in this is, um, interesting.

Henry Spencer at U of Toronto Zoology

## Thoreau and Navigation (Harper, RISKS-8.56)

Eric Roskos <roskos@ida.org> Mon, 17 Apr 89 13:04:31 E+

Thoreau had a considerable interest in this subject, actually. In one of his earlier works (I think "The Maine Woods") he tells in great detail the story of the incident he's probably referring to here, in which a ship split open after colliding with a rock called "The Grampus" ("grampus" being the name of a kind of whale, the name coming from the Latin "crassus pisces," or "fat fish"). He saw a large sign that advertised the disaster like a circus poster, and he and his brother turned aside from their trip to go see. He ends up the story with the moral "The resolute man's purpose cannot be split on any grampus," which was the cryptic quote in my signature line for a long while on the Usenet, back when we subscribed to it here.

It is good to see someone reading Thoreau; he had a lot of comments on the progress of technology, and had a great appreciation of telegraph wires for reasons other than merely the fact that messages were sent down them.

"... we will see that some will be riding, and the rest will be run over; and it will be called, and will be, `a melancholy accident'."

[His comment on public enthusiasm for new technology, and the fact that often in the end it turns out not to be that useful, and sometimes harmful, for many of the people who were most enthusiastic about it. In this case, he was talking about the new steam locomotive that was coming to Concord.]

#### Risks of automatic order entry in restaurants

Daniel Klein - 412/268-7791 <dvk@SEI.CMU.EDU> Mon, 17 Apr 89 00:28:06 EDT

Last week I had the pleasure of eating in one of those restaurants that has an

automatic order entry system. This is a system whereby the waitroid has a hand held terminal onto which s/he enters the table's order, and this order is relayed via infra-red to a pickup in the ceiling, thence to the central order computer, and finally to the chefs in the kitchen. It is a marvelous system, as long as it works.

In this case, the chef stolidly maintained that he never received one of our orders. Since the computer had not told him to service an order, he refused to do so. The waiter was unable to convince him. Similarly, the waiter refused to resubmit the order, since his terminal informed him that it had been processed, and if he resubmitted the order, he would be liable to collect double the fare.

We waited for over two hours for our food, until we advised him that the hand-held terminal would find a very uncomfortable location on his body if \*we\* got our hands on it :-) It took the intervention of the manager to get the food (and why it took 2+ hours, I will never know).

In the end, the waiter apologized to us, graciously explaining that it was a "computer error" that had caused all the delay.

-Dan

## ✓ Re: Most Accurate Clock (RISKS-8.56)

<uunet!microsoft!clayj@lll-winken.llnl.gov> Mon Apr 17 08:35:05 1989

Here's a followup to the article I sent last week about HeathKit's "Most Accurate Clock" and Daylight time.

After my problems with the clock being exactly 1 hour off, I checked with both Heath and NBS (the folks who run WWV/WWVH) and discovered that the embedded digital signal does indeed include a packet which indicates Daylight time.

The decision to send the packet is controlled by a manual switch at the WWV site in Ft Collins. According the NBS, "...our people don't make mistakes when using that switch..(paraprhased)". According to Heath, "We've had several complaints about this over the years".

I'm certainly glad that I don't have anything depending on the correct hourly readout from that clock! (although I do have my computer system set up to set it's time from the clock once a day).

Clay Jackson, Microsoft

### Fuel Management/Mis-management

Brown <mlbrown@nswc-wo.arpa> Thu, 13 Apr 89 16:41:48 EST

The discussion on the Boeing fuel management issue reminds me of an issue that we delt with when I first came to work here at NSWC. The first A6-E aircraft

delivered to the Navy had severe fuel management problems. In fact, the first A6-E I saw we dug out of the swamp near Norfolk VA. The A6E has two wing tanks and a main tank behind the cockpit. However, to be used, the fuel in the wing tank must be pumped into the main tank from which it is pumped into the engine. The pilot took off with an indication of a full main tank and full wing tanks. During ascent, the engines flamed out. The pilot suspected that the main tank was empty and started the transfer from the wing tanks to the main. However, the pumps were not fast enough and he could not restart the engines. The problem was a failure prone fuel level indicator. The advantage that a computer would have added is that it would have made the same error that the pilot did - assuming that the indicator was correct. Therefore, we can still blame the pilot for not checking the tank prior to take-off.

Mike Brown

### Companies mask ANI to calm callers

<use><USER=GEBM@um.cc.umich.edu>Sat, 15 Apr 89 15:53:18 EDT

The following condensed from Bob Wallace, Network World v6#7 2/20/89 pg 1.

Fear of alienating customers has encouraged some companies to rethink the way they use ISDN's automatic number identification (ANI) capability.

American Express Travel Related Services Co. (TRS), AT&T's first commercial ISDN user, reportedly found that customers were startled when some of its agents greeted them by name. TRS has since prohibited the practice. Richard Zatarga [TRS employee], in a presentation at a "Preparing for ISDN" conference in Toronto (12/88), said TRS now avoids identifying callers by name. "We have changed the way we answer the [telephone]. We know who they are, but we still hunt for information" from callers as if we had to identify them.

Although TRS has since denied that it used ANI to identify callers by name and that it received negative feedback from cardholders, sources close to the project who requested anonymity said numerous users reacted unfavorably to personalized greetings. TRS "learned that you don't answer the telephone with the customer's name."

American Transtech, a wholly owned subsidiary of AT&T (and the first company to test ISDN Primary Rate Interface [32B+D]), processes one million calls a day, making it the nation's fourth largest telemarketing company. The company does not, however, greet callers by name. "We could do it, but we don't want to let customers know we can capture their telephone number," said a spokesman. "We don't use [specialized greetings] because it would intimidate callers."

Besides the RISK of alienating customers with ANI, there is a pervasive fear among prospective ANI implementors that callers will raise legal objections to ANI once they know how it works. People with unlisted phone numbers are expected to spearhead that movement.

According to Huel Halliburton, a communications manager with Centel Electric, central office switches equipped to support equal access deliver the phone

numbers of callers with both listed and unlisted telephone numbers to companies that use ANI.

### ★ The dangers of electric windows

<"Martin\_Cooper.osbunorth"@Xerox.COM> 15 Apr 89 14:54:22 PDT (Saturday)

J M Hicks' contribution on Central Locking Systems (RISKS 8.55) brings to mind many other potential dangers of electrical control in autos. Most of these I have seen discussed at various times within this forum, but there is one in particular which concerns me.

Electric windows are becoming ubiquitous on new cars today, and unlike central locking systems, there is no manual override. This is made very obvious by the fact that such windows cannot be raised after the ignition has been turned off, which is in itself a rather annoying attribute.

However, annoyance turns to danger when an emergency arises. In an auto accident causing the doors to jam closed, the windows are the only means of escape when waiting for a cutting crew could be fatal. Furthermore, it is well known that the windows provide the best (only?) means of escape from a car underwater. If the electrical system is shot, and the occupant is unable to break the windows, what other options are there?

Certainly electric windows provide a great convenience in everyday driving, but I wonder how many people consider the risks when they choose their options on a new car. And I wonder if the auto manufacturers themselves realise the risks and are merely cutting costs because nobody voices concern.

Martin F N Cooper, Xerox Corporation

## Careless tape transfer procedures

Peter Jones <MAINT@UQAM.BITNET> Sun, 16 Apr 89 12:00:33 EDT

This morning, walking in a public area of a building, I noticed a messenger or computer operator ahead of me in the same corridor casually wheeling an open cart loaded with about a dozen tapes. Suddenly, he left his cart in front of an overhead door, walked on about 50 feet to the next door off the corridor, and disappeared. Curious, I waited in the vicinity of the cart to see what would happen next. Some 30-60 seconds later, the overhead door opened, and the clerk appeared from behind, pulled the cart in, and closed the overhead door again. I continued on my way, with a few questions turning over in my mind:

- 1) What if someone had made off with a tape or two while the cart was unattended?
- 2) Why wasn't the messenger accompanied by, say, a security guard with a radio? The guard could have watched the cart while the messenger went to open the

door. Also, this precaution would avoid the risk of the messenger being attacked by a gang (2 or 3 would be enough to steal a tape or two) while passing through the public areas.

- 3) Why weren't the tapes in an enclosed box, locked with a key at the beginning of the trip, and unlocked with a duplicate at the destination. (The messenger, of course, should not carry a key!) This would prevent tapes from disappearing or being substituted while in transit.
- 4) Do people still do stupid things like this in 1989? (Yes!)

Peter Jones MAINT@UQAM (514)-282-3542



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 8: Issue 59

Tuesday 18 April 1989

## Contents

- More on the British Midlands 737 crash **Robert Dorsett**
- Computers and Food Poisoning [anonymous]
- The dangers of electric seatbelts (was: windows) Clements
- Re: The dangers of electric windows **Daniel Klein**
- Newspaper Cartoons and Computer Infallibility G. McClelland
- Re: Thoreau and Navigation David A Honig
- "Journalist Vigilantes"

Walter Roberson

- Hazards of RF near electronic controls **Dana Myers**
- Info on RISKS (comp.risks)

#### More on the British Midlands 737 crash

Robert Dorsett <mentat@dewey.cc.utexas.edu> Tue, 18 Apr 89 14:47:36 CDT

The following editorial appeared in the 1 April 1989 issue of FLIGHT INTERNATIONAL. It seems to indicate that a bevy of old, controversial issues are bubbling to the forefront again: technical training for pilots, cross-type ratings, cockpit design, EROPS reliability, and computer-assisted information systems.

In the hours that followed the crash of a British Midland Airways Boeing 737-400 on Britain's M1 motorway, the airline industry harbored fears that the accident held terrible significance for the burgeoning business of flying twinjets for long distances over water.

Dual engine failure was soon ruled out as a cause of the British Midland

crash, but with last week's publication of its special bulletin on the accident, the United Kingdom Air Accidents Investigation Branch has raised new issues with equal significance to extended- range operations (EROPS). ...

What possible significance can the crash of a short-haul airliner on a hop from London to Belfast have to the safety of aircraft crossing and recrossing the world's oceans?

While the AAIB's special bulletin makes no attempt to determine the accident's cause, or to apportion blame, it details a sequence of events which could easily have occurred in mid-ocean, with equally disastrous results.

The sequence begins with the failure of a fan blade in the 737's left engine, producing symptoms which the crew wrongly diagnosed as a problem with the right engine. Those symptoms included vibration, plus smoke and the smell of burning carried by the air conditioning in the cockpit.

After examining systems recovered from the crashed aircraft, the AAIB is certain that the cockpit instruments correctly indicated severe vibration in the left engine. Investigators note, however, that pilots distrust aircraft engine vibration indicators, based on experience with earlier electromechanical instruments. Crews seem unaware that electronic indicators on later 737-300's and the 737-400 are more accurate.

Another example of mythology triumphing over knowledge is the apparent perception among 737 crews that cockpit air conditioning comes solely from the right engine, and that smoke and burning smells in the cockpit tend to indicate fire in the right engine. In fact, air supplied to the cockpit comes from both engines, in a 70:30 right: left mix.

Whether either of these misconceptions played a part in the British Midlands crash is not addressed in the AAIB's special bulletin, but FLIGHT understands that accident investigators have become increasingly concerned at the level of technical knowledge expected of airline pilots.

The issue of technical knowledge takes on new significance in a two-crew twinjet flying 1200 nm from the nearest airport. Theoretically, the information systems in modern widebody airliners should provide the crew with everything they need to know, and prompt them to take timely and correct actions to cope with any emergency. This assumes that the crew understands, and trusts, what the system tells them, however.

In mid-ocean, a high degree of mutual man-machine trust is essential. Information supplied to the crew must be trustworthy--and be known to be trustworthy--and knowledge must triumph over crew mythology. That means better technical training for pilots. The alternative for safe EROPS is to reintroduce that much-maligned breed, the flight engineer.

Three months after the M1 crash, the AAIB is still piecing together what happened on Flight BD092, despite having ready access to the crew, the wreckage, and good recorded flight data and cockpit voice. It will be months before the final accident report is published.

If an EROPS aircraft goes down in mid-ocean, what the cause might never be discovered" (sic).

#### Computers and Food Poisoning

<[anonymous]> Tue, 18 Apr 89 11:07:37 PDT

A controversy is currently before Congress over a Dept. of Agriculture plan to cut in half (from around 2000 to around 1000) the number of meat plant government inspectors. Part of the rationale for this change (which is being protested by numerous consumer watchdog groups and many meat inspectors themselves) is that a new computer system allows for very precise "targeting" of the plants which are most likely to have problems, thusly (supposedly) allowing for fewer visits to plants the computer considers "safe" based on various parameters (including past history, etc.)

However, in testimony before Congress, current inspectors have (at risk to their own jobs) testified that the computer system being used is not reliable. Reports have indicated that it makes mistakes about even very "simple" data items, including sending inspectors to plants when they are closed. This certainly doesn't raise one's hopes about the more complicated data factors the system must also handle! One inspector pointed out how the computer forbid him going to a particular plant because the model deemed that plant "safe". But based on his own knowledge, he went there anyway, and found serious food poisoning contamination.

Most watchdog groups feel that we need MORE meat inspectors, not less. For the federal government to use questionable computer models as an excuse for slashing meat inspection seems to show extremely poor judgement and a considerable risk.

Anyone for a burger?

[If you do eat meat, support your friendly natural meat producers. The computer model undoubtably ignores growth hormones, dyes, antibiotics in the grain feed, etc., even at dangerous levels. By the way, whistleblowers seem to deserve some anonymity, for otherwise the watchdog might get turned into a hotdog. (Bribing the inspector with free drinks might be called 'Wetting your Whistleblower'.) PGN]

### ★ The dangers of electric seatbelts (was: windows) (RISKS-8.58)

<clements@BBN.COM>
Tue, 18 Apr 89 15:21:06 -0400

On my last vacation trip, I rented a car with "Automatic Seat Belts". In this particular car, at least, these have a very powerful motor and no manual override once they start moving. I found them really scary.

When I commented on them while returning the car, the agent said (paraphrased):

"Yeah, they're pretty bad. We had one catch a lady's earring in the belt and it ripped part of her ear off."

### ★ Re: The dangers of electric windows [RISKS-8.58]

Daniel Klein - 412/268-7791 <dvk@SEI.CMU.EDU> Tue, 18 Apr 89 11:16:04 EDT

One nice thing about driving an Alfa Romeo (which has power windows) is that in my 1978 model, a hand crank was provided as a manual override to the power motor (the crank was stored in the glovebox). The newer models don't have this feature since, according to the mechanic, the window motors just never went bad (I'll believe him - my 1987 has had \*nothing\* go wrong anywhere on the entire vehicle).

Of course, in the event of a water landing, I will simply pop the roof and punch out vertically. And they tell me the Alfa isn't a practical car! :-)

-Dan

## Newspaper Cartoons and Computer Infallibility

<MCCLELLAND\_G%CUBLDR@VAXF.COLORADO.EDU>
Tue, 18 Apr 89 07:39 MST

From today's Hi & Lois newspaper cartoon strip:

Clerk [to Hi]: I'm afraid we're out of stock on that item, sir.

Hi: I found it on the rack. I just want to buy it.

Clerk: Sorry, but we can't sell something the computer says we don't have...

[More like Hi and Dry! PGN]

## Re: Thoreau and Navigation

David A Honig <honig@BONNIE.ICS.UCI.EDU> Tue, 18 Apr 89 08:30:05 -0700

- > It should be borne in mind, however, that Thoreau was speaking of the
- > tables calculated by HUMAN calculators, not machines. ...

Agreed, the tables were computed by humans, but then, who writes software, who designs hardware? :-)

The general issue is: What are the risks involved in trusting one's artifacts, whether they are instruments, tables, computational theories, algorithms, machines, etc.?

## "Journalist Vigilantes"

<Walter\_Roberson@carleton.ca>
Tue, 11 Apr 89 20:11:17 EST

An article by Gary Marx, in the local weekend paper, but apparently reprinted from The Christian Science Monitor, discusses the trend towards TV news shows using videos filmed by amateurs with video recorders. The article, entitled "\Bold{Cower!} You're on candid camcorder" in the local edition, mentions several points quite familiar to long-standing RISKS readers (eg, "It is possible to create images not found in reality and to mix real and imaginary images,"), but is interested as one of few publically newspaper articles that concern themselves specifically with the risks to privacy that technology can easily bring about. Some parts extracted from the article:

'Information technology in private hands can offer documentation and alternative views. [...]

Without appropriate policies, there is a danger of creating a group of journalistic vigilantes who will offer fraudulent or contrived news, invade privacy, and debase the quality of television news. [...]

Camcorders are at least visible, but tiny hand-held video cameras the size of a deck of cards can also be purchased along with cameras hidden in picture frames, mirrors, briefcases, and even books.

Our lives may increasingly become episodes in someone's version of \it{Candid Camera}. [...]

Video cameras must be considered alongside other potentially invasive information technologies such as miniature voice-activated tape recorders, devices for remotely monitoring telephone and room conversations, computer dossiers, electronic location monitors, and drug testing. [...]

These new technologies are likely neither to be as harmless as advocates claim nor as dangerous as critics fear. Their impact will be determined not by anything inherent in the technology but by the choices we make."

-- The Ottawa Citizen, Sat. Apr. 8, 1989, pg B6

[The trailer notes that Gary Marx is the author of \it{Undercover: Police Surveillance in America}. ...]

Walter Roberson < Walter\_Roberson@Carleton.CA>

#### Hazards of RF near electronic controls

Dana Myers <dana@bilbo.LOCUS> Wed, 12 Apr 89 11:51:50 PDT

Dave Horsfall writes:

> (my 2m HT has) just 3 watts and a rubber ducky... very inefficient

Well, it may not be really efficient at getting your signal anywhere far, but a short antenna like that can have very high RF voltages present. I know my Kenwood TR-2600 (1 or 3 Watts between 144-148 MHZ) would easily reset the telephone on my desk before we upgraded to a Rolm system, which appears to be resistant. It isn't the power that upsets electronic devices - it usually is the voltage. There may be parts of an electronic control which resonate at high frequencies, and therefore build up large levels of voltage, enough to force a low logic level high, etc. It is hard to foresee that in the design of a system which is intended to operate at much lower frequencies.

The Otis 401, though it did malfunction, also detected the malfunction before doing anything dangerous. This is a case where the designer could not prevent RF from upsetting the controls, but did build a mechanism to gracefully cope with the upset. Even if the control was encased in an RF tight box (which would likely increase the cost significantly), the ability to cope with RF or EMI induced upset must be there. Since it isn't often that the control will be inundated with RF at close range, the design need really only cope the infrequent case that upset occurs.

Dana H. Myers, WA6ZGB, Locus Computing Corp., Inglewood, CA



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 8: Issue 60

# Wednesday 19 April 1989

## Contents

- Hillsborough: Risks of using Computers at Stadium Turnstiles **Brian Tompsett**
- Risks of plaintext data **Hugh Miller**
- Computer voting at Stanford Scott Seligman
- Re: Computerized attendance Sean Fagan
- More Auto-Seatbelt Horrors **Thor Simon**
- Mb = 1024? 1000?

Walter Roberson

- Re: Newspaper Cartoons and Computer Infallibility Will Martin
- Info on RISKS (comp.risks)

### ★ Hillsborough: Risks of using Computers at Stadium Turnstiles

Brian Tompsett <bri>hriant@SPIDER.CO.UK> Wed, 19 Apr 89 14:03:13 -0100

Heard on BBC radio Parliamentary report this morning. At question time a Member of Parliament stated that the Police at Hillsborough based their decisions to open a gate on the computerized tally from the turnstiles that indicated the ground had ample space to take more people. The government's plans to make computerized turnstiles compulsory increases the risk that a computer failure or error could result in another tragedy in the future. The government where asked to reconsider their plans in the light of recent events.

Brian Tompsett. Spider Systems Ltd, Edinburgh.

#### Risks of plaintext data

Hugh Miller <MILLER@vm.epas.utoronto.ca> Wed, 19 Apr 89 16:09:41 EDT

Excerpted from "MP demands probe into burglaries," by Tim Harper, \_Toronto Star\_, We 19 Apr 89, p. A13:

OTTAWA - A New Democrat MP has asked for an investigation of a series of "high quality break-ins" at his office and those of 4 environmental and peace groups. Jim Fulton said yesterday the break-ins preceded the grilling of a senior defense department scientist in a probe to flush out the person who leaked information about nerve-gas testing in Alberta ... No one was arrested and the RCMP have rejected any link.

Kirk Roberts, a spokesman for the Ontario Environment Network on Spadina Ave., said thieves who ransacked the office Jan. 13 stole equipment but ignored a personal computer valued at \$3500. The thieves, Roberts said, were interested in stealing data tapes that included correspondence among some 100 Canadian environmental groups ...

In a letter to Fulton about the break-ins, RCMP Commissioner Norman Inkster wrote, "Our enquiries into this matter have not uncovered any evidence to suggest the incidents were linked or conducted by any organized group of individuals."

I spoke with Kirk Roberts this afternoon. "I've got to get hold of this article," he said. "I don't know what the thieves were \_interested\_ in, but they in fact did steal all of our backup tapes, except for the ones we keep off-site."

OEN uses a WEB system, which provides dialup connections to 47 countries and affords full email/messaging functions. The system utilizes 120MB tape cassette backups. "The system does afford an encryption option for users who want to use it," said Roberts. "But the thing is, none of the stuff on those tapes was what you would call particularly sensitive. If any reasonable request had been made for items on those tapes, we would probably have supplied them. As an environmental organization we do things, and \_want\_things done, publically. That these tapes were stolen says more about the thieves' paranoia than about the tapes' contents."

OEN has only suffered the one break-in so far, said Roberts. Jim Fulton's Parliament Hill office has, however, he hears, been burgled four times.

Hugh Miller, University of Toronto

## Computer voting at Stanford

Scott Seligman <seligman@polya.Stanford.EDU> Wed, 19 Apr 89 00:12:55 -0700

This year, for the first time, students voting in the student elections here at Stanford University aren't using paper ballets or voting machines. They're using Macintosh computers.

People have been making quite a big deal out of this. The papers report that

state officials are observing the process. Past student elections have been plagued with administrative bungles, which the computers are supposed to help prevent. The whole thing is quite important to the people who are administrating it -- one would think that they've been extremely careful....

I went to vote today. After I had cast all of my votes, a window appeared asking me if I now wanted to make my selections permanent. Seemed reasonable enough. But there was only one possible response to click on: "No". As this wasn't the response I was hoping to make, I hit return and clicked a few times and the window went away and then it came back again. This time there were two possible responses: "Yes" and "No". I selected "Yes", confident that my votes were being accurately recorded.

(I'll leave it to others to report on the numerous machines out of service, and the long queues at the ones in service, and the complete lack of privacy, and ....)

[While this system is a nice advance in letting the voter review the ballot, the problems of system integrity, assurance of nontampering, ballot privacy, etc. are largely ignored. It is certainly a worthwhile experiment, and will provide challenges for system penetrators and authorized programmers who want to rig elections. Some of the problems that will need to be overcome have been discussed extensively in the reports by Roy Saltman, Lance Hoffman, and others mentioned in earlier RISKS. PGN]

## ★ Re: Computerized attendance (RISKS-8.57)

Sean Fagan <seanf@ucscc.UCSC.EDU> Wed, 19 Apr 89 03:59:23 -0700

We had one in our high school, similar to a combination of the above [described in RISKS 8.57]. Each student had an 8 digit number (birthday, plus 2 digits for repeats; never mind the RISKS in that!), and the 2nd period class would fill out a little bubble sheet, which had 'present,' 'excused,' 'absent,' and 'tardy.' These would then be scanned, processed, and an absent child would have his (or her) parents called that evening. A child who was tardy for more than 3 days in a row, or for more than 20 days in a semester, would also have her (or his) parents called.

I should mention that I grew up in a largely hispanic neighborhood, and they never did figure out how to handle the cases where the parents understood only English or Spanish (they tried English only, didn't work; tried Spanish only, my mother threw a fit 8-)). Nor did they take answering machines into account...

Oh, of course, an obvious RISK: the computer originally was called up by a central computer in LA (Los Angelos) to send various reports. It took me and my cohorts 2 weeks to find out the number of the computer, after which we demonstrated how much we could screw up the system merely by calling repeatedly (keeping it busy) (yes, we told people what we were doing; they didn't believe us till we showed them [they were present when we were doing it, ok? 8-)]). Shortly after that, they changed to having the computer call LA, which was a

number we never did figure out...

Sean Eric Fagan (408) 458-1422

### More Auto-Seatbelt Horrors [RISKS-8.59]

Thor Simon <simon@cheshire.cs.columbia.edu> 19 Apr 89 02:04:17 GMT

In response to the recent post on the dangers of automatic seatbelts:

One day, while my father and I drove along in a rental car (I believe a Subaru) with automatic seatbelts, he saw that he'd caught his coat in the car door. Of course, being me, I dared him to open it and see if it fell out. He opened the door, and much to our surprise, the seatbelt opened, all while happily motoring along at about 40. Later that day I looked it over and saw that the seatbelt-opener used a simple pressure switch that could have been lifted intact from any refrigerator-light mechanism. Needless to say, this is VERY dangerous. Scenario:

John and his buddies go for a ride. Being saftey-concious, He owns a car with auto-seatbelts. Unfortunately, they need them. They are sideswiped by a giant Mack truck. More unfortunately, the driver's side door \_pops open\_. This triggers the seatbelt-release mechanism, John hits the windshield and...

Not fun, huh? Well, at least it looks like such seatbelt improvements may be obsoleted by the new \$30 airbags... I hope.

Thor Simon

#### ✓ Mb = 1024? 1000?

<Walter\_Roberson@CARLETON.CA> Wed, 19 Apr 89 12:57:18 EST

I found this is a SunSpots Digest we received today (v229). [How do you stick your thumb in to check how full a file system is? :-) ] Walter Roberson

```
> Date: Tue, 28 Mar 89 07:45:08 CST [...]
```

- > I know that once I was unpleasantly surprised when I planned on a 512 MB
- > file systems size and calculated what that should be in terms of sectors
- > and cylinders on my disk. I figured that 512 MB = 512 \* 1024 \* 1024 =
- > 536,870,912 bytes. When I made the file system, I found out it was not 512
- > Mb (from the output of newfs). Working backwards, I found that Sun used
- > 512 Mb = 512 \* 1000 \* 1000, which makes [sense] to me since I am a
- > mechanical engineer, but we all found it confusing.

>

- > Dinah Anderson
- > Shell Oil Company, Information Center (713) 795-3287
- > ....!{sun,psuvax,soma,rice,ut-sally,ihnp4}!shell!dinah

[An old problem. But since we haven't had it in RISKS since volumes 2 and 3, it might as well resurface once again. PGN]

## Re: Newspaper Cartoons and Computer Infallibility

Will Martin -- AMXAL-RI <wmartin@ST-LOUIS-EMH2.ARMY.MIL> Wed, 19 Apr 89 14:39:34 CST

- > From today's Hi & Lois newspaper cartoon strip:
- > Clerk [to Hi]: I'm afraid we're out of stock on that item, sir.
- > Hi: I found it on the rack. I just want to buy it.

Too bad they didn't follow that with the obvious:

Hi: Well, since you don't have this, this can't be yours. It must be mine. [Walks out of store with item for free...]

[But they'd probably be searching Hi and Lois. 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 8: Issue 61

Thursday 20 April 1989

#### Contents

Alleged Computer-aided fraud

**Rodney Hoffman** Black box for automobiles

**Anthony Stone** 

References to smoking and computer failure?

David A Rasmussen

The danger of testing (re RFI and elevators)

Dave Collier-Brown

Reaction to John Luce's letter on electronic elevators

Peter Jones

Industry not protecting privacy

**Rodney Hoffman** 

Sun386i security problem update **Ed DeHart** 

Writing on "write-protected" disks David M. Zielke and Peter Jones

Info on RISKS (comp.risks)

#### Alleged Computer-aided fraud

Rodney Hoffman < Hoffman. El Segundo @ Xerox.com > 19 Apr 89 10:22:50 PDT (Wednesday)

Summarized from a story by Gregory Crouch in the 'Los Angeles Times', 18-April-89:

A whistle-blower alleges that Litton Systems designed a company software system to under-record the computer usage of Litton's commercial clients, causing the federal government to be over-charged. Former Litton employee James Carton has filed suit after concluding that Litton rigged its computer billing service to over-charge the government more than \$25 million between 1983 and 1988 for computer work on hundreds of defense contracts. Late last month, the U.S. Justice Dept. announced that it has taken over Carton's suit. With fines for every instance of over-charging and treble damages, the total could reach \$175

million. Under the False Claims Act, Carton stands to receive 15% to 30% of any damages awarded to the government.

Litton denies the charges, claiming it saved the government money by letting commercial customers use the same computers.

While writing an assigned report on the profitability of Litton's computer services, Carton noticed that most of the commercial customers, accounting for more than half of the data center's revenue, were actually costing the company money. One company was charged for using two disk drives when it actually was using three. At the same time, the government was being overcharged. He discovered and reported more discrepancies, but, more than a year later, nothing had changed. He finally decided to file suit.

#### Black box for automobiles

Anthony Stone <stone@nbc1.GE.COM> Wed, 19 Apr 89 17:43:08 edt

>From "World Press Review," May 1989, quoting "Wirtschaftswoche," Duesseldorf:

A "black box," or data recorder, for cars is being developed by a consortium in West Germany. The size of two cigarette packs, it will cost \$215 and record changes of direction, the status of lights and turn signals, steering-wheel and pedal positions, and even whether the radio is on. Every 30 seconds new data will be stored on a microchip; in an accident, this data will freeze, and later information will continue to be recorded...

[Once again, there is a serious question as to the integrity of the data in the recorder. In a court of law, we have the problem that the data may not be what was recorded in real-time... PGN]

### references to smoking and computer failure?

David A Rasmussen <dave@csd4.milw.wisc.edu> Wed, 19 Apr 89 19:53:09 -0500

A colleague of mine in county planning is having trouble convincing people not to smoke next to computer systems containing supposedly irreplacable info, and is worried about tar and nicotine buildup on disk drives. Any suggestions?

[Use digital filters? Responses to David, please. PGN]

### The danger of testing (re RFI and elevators) [Horsfall, RISKS-54]

Dave Collier-Brown <dave@lethe.UUCP> Wed, 19 Apr 89 21:23:44 -0400 [The foregoing discussion] raises a computer version of a well-known risk: that of testing for errors. (Not to mention the risk of finding and/or reporting them!)

Almost any test of any piece of equipment is definable as trying to make the equipment fail.

If it does fail, the person doing the testing is liable to civil or criminal penalties.

If it does not, she risks being subject to lesser penalties for trying to make the equipment fail.

This is an interesting double-bind (well, 1.5-bind actually) that can be used to discourage testing of potentially dangerous things. Because it typically requires some kind of legal protection for the tester, it is often held to be something only a government should do. Yet if it is, then we are faced with finding out how to test the testers who are acting as our agents...

It can also make ordinary people reluctant to run \*\*necessary\*\* tests.

Well before the Internet Worm of yore, I executed a uucp-test program named "virus" that informed system managers if their security was unnaturally low. As you might guess, some were concerned. Regrettably, some took exception to the fact that the test was done \*\*at all\*\*, and called upon my management to ensure that their opinions would be made known to me. (In my Honeywell days this sort of thing was known as a "career killer").

In fairness I should point out that some people knew a test program on sight and publicly defended the test, the program and myself. (Thanks, Dave and Erich!)

Nevertheless, the chilling effects were real. And the problem of protecting the testers is still outstanding.

--dave (I survived, obviously) c-b David Collier-Brown, 72 Abitibi Ave., Willowdale, Ontario, CANADA. 223-8968

#### Reaction to John Luce's letter on electronic elevators

Peter Jones <MAINT@UQAM.BITNET> Thu, 20 Apr 89 14:02:07 EDT

John Luce's comments on the design goals of electronic elevators certainly raised the level of my knowledge about them. I would like to offer some comments:

1) Automatic systems should not outguess the user and do unexpected things without an explanation at the time of occurrence. I am referring to the fact that, after the doors are held open for a length of time, a car sometimes has to go to a specific place to initialise itself. This behaviour is disconcerting, and can be frightening to a person who is afraid of elevators. The recorded announcement could be used to tell the user what is

happening and thus reassure him.

Arbitrarily cancelling the buttons inside the car is not foolproof. What about a group of small children, each going to a different floor? How would a blind user know about the cancellation? A better solution would be a specially-shaped button inside the car (maybe you'd pull instead of push) that would allow someone getting in an car with no-one inside to to cancel the uselessly selected floors.

Sometimes it's desirable to be able to select a floor that's in the wrong direction. For example, in many buildings, especially apartments, the call buttons outside only go one way (down). For a trip upward, you have no choice but to select the wrong way. Also, if a large number of people (several cars full) want to make the same trip, it is useful for people in the first cars to send them back for more.

2) The elevator m	anufacturer was wrongly blamed for features that were the
building owner's	responsibility. I have yet to see an elevator where the
division of respo	onsibility is spelled out for the user (e.g. a sign saying
"If you have any	comments or complaints about the audio announcements,
please contact _	, and not Otis."

Peter Jones MAINT@UQAM (514)-282-3542

## Industry not protecting privacy

Rodney Hoffman <Hoffman.ElSegundo@Xerox.com> 19 Apr 89 17:47:21 PDT (Wednesday)

An article by Jim Schachter in the 'Los Angeles Times' 19-April-89 is headlined U.S. INDUSTRY DOES A POOR JOB OF PROTECTING PRIVACY, STUDY SHOWS. Univ. of Ill. Prof. David Linowes chaired the U.S. Privacy Protection Commission more than a decade ago. He has now released a new study showing just how little attention has been paid to the commission's conclusions and just how much ground has been lost. He urges Congress to act. Prof. Harley Shaiken of UC San Diego calls for "applying the standards of the Bill of Rights to the workplace."

Linowes says outdated, inaccurate records are being used to make critical decisions about hiring and promotions. "This information is never destroyed, and it's obtainable instantaneously." State and federal privacy laws remain a patch-quilt, and advances in computer and telecommunications technology have increased data collection and analysis.

According to the new survey of major corporations, 38% still have no policy on releasing employee records to government agencies, and 57% do not tell employees what records about them are maintained. 42% gather data about workers without telling them, and 57% hire private investigators to probe employees' or job applicants' backgrounds.

A sidebar lists PRINCIPLES OF A 'FAIR INFORMATION' POLICY:

- 1. Minimize intrusiveness. Don't collect more data than is necessary.
- 2. Maximize fairness. Let the subject know what information is being collected and why.
- 3. Establish an enforceable expectation of privacy. Provide recourse if privacy is violated.

### Sun386i security problem update

<ecd@SEI.CMU.EDU> Thu, 20 Apr 89 14:32:39 EDT

The serious security problem that was reported in <u>Risks Volume 8</u>, <u>Issue 15</u> has been corrected by Sun. Sun support and Sun's field offices are now able to supply a new set of programs that will solve the problem. We strongly recommend contacting Sun A.S.A.P.

Until you receive the new programs from Sun, we suggest that you change the protection of the login program.

chmod 2750 login

This will allow login to continue to work but removes users access to it.

Since we do not have a Sun 386i system at CERT, we were unable to test the new programs being supplied by Sun. Field reports indicate that the new programs do solve the problem.

Thanks, Ed DeHart,
Software Engineering Institute / Computer Emergency Response Team, 412-268-7090

[Sun fix also noted by gww@Sun.COM (Gary Winiger). PGN]

### Writing on "write-protected" disks

<Info-IBMPC@WSMR-SIMTEL20.ARMY.MIL>
Wed, 19 Apr 89 20:04:22 BST

When using floppies, the user is generally led to beleive that nothing can happen to alter a floppy that lacks the notch giving permission to write. In actual fact, this is not the case. For example, the APPLE II inplemented the protection of diskettes in software. Worse still, in the case of the APPLE, was a failure (observed by the author on at least two systems) of the drive electronics whereby the heads would be "on' continually, and thus degauss random spots on the floppy (while the head was moving) and all of one track (when the head stopped moving, generally on the boot track!) on any disk inserted! At an Apple club here in Montreal, members were warned to try their Apple with a working diskette with no critical files, then a backup copy of that if the first failed, then to DO NOTHING ELSE if neither worked. That way, at worst you would only risk degaussing two virgin copies of a working disk, and not, say, a \$300 copy-protected software package or irreplacable data. I had always thought the problem was unique to the Apple. However, the following

item, from Info-IBMPC Digest, shows that this is not the case. Do RISKS readers know of other systems that are not protected at the hardware level? What about 3 1/2 "rigid floppies"? What about magnetic tapes? Cassettes?

Peter Jones MAINT@UQAM (514)-282-3542 -----Original article follows: ------

Info-IBMPC Digest Wed, 19 Apr 89 Volume 89 : Issue 41

Today's Editor:

Gregory Hicks - Chinhae Korea < COMFLEACT@Taegu-EMH1.army.mil>

Today's Topics:

..

Possible to write to a "Write Protected" Disk

···

Date: 10 Apr 89 17:44:00 CST From: zielke@physics.rice.edu

Subject: Possible to write to a "Write Protected" Disk

In reference to the sure fire cure for viris problems using a bootable disk in drive A which is "write protected". This write protection is performed in software at some level. It is possible "At least on a Real IBM-AT 6mhz, first rom revision" to write directly to the disk and bypass the write protect mechanism. I do not know how it was done but I know that it can be done, I ran across someone who had written this code so as to be able to write on disks with no notch cut in them...

David M. Zielke

ARPA==> Zielke@Physics.Rice.Edu
Zielke@128.42.9.23

MaBell==> 713-527-8101 ext. 4018 work
713-666-2982 home

US Snail==> David M. Zielke, 7490 Brompton #110, Houston, Tx 77025



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 8: Issue 62

Monday 24 April 1989

## **Contents**

Release SkyDome, Release 0.0

**Mark Brader** 

Risks of plaintext data (II)

**Hugh Miller** 

Computer orders for phone books

Mark Brader

ATM's used to track accused killer

Al Stangenberger

Computer Voting

**Chris Davis** 

Re: Most Accurate Clock

**David Schachter** 

Writing on write-protected disks

Leigh L. Klotz

Kenneth R. van Wyk

Phil Goetz

**Dimitri Vulis** 

**Henry Spencer** 

**Dave Kemp** 

**Rich Sims** 

Info on RISKS (comp.risks)

## ✓ Release SkyDome, Release 0.0

Mark Brader <msb@sq.sq.com> Thu, 20 Apr 89 21:02:09 EDT

Today's Toronto Star also has an article about the SkyDome. That's the city's new stadium, the world's first with a retractable roof using rigid segments. According to the article, when the stadium opens this summer, the roof will operate at 1/3 speed, taking an hour to open. And the reason for this is that the computer programs to work it aren't ready and a "smaller" version will be in use.

Mark Brader, SoftQuad Inc., Toronto, utzoo!sq!msb, msb@sq.com

[This of course contradicts the myth that smaller programs run faster. PGN]

### Risks of plaintext data (II)

Hugh Miller <MILLER@vm.epas.utoronto.ca> Fri, 21 Apr 89 09:23:48 EDT

The "information break-ins" story posted two days ago has become front-page news in the \*Toronto Star\* today ("Who stole files in mystery break-ins?" by Tim Harper, Fr 21 April 89. p. A1). Here is a chronology, extracted from the article:

- 21 Nov 88 University of Toronto campus offices of Science for Peace: floppy disk containing membership address list, financial records, correspondence, drafts of communiques, and a work in progress by George Ignatieff, former chancellor of the university and Canadian UN ambassador, on the use of chemical weapons. Nothing else touched.
- 13 Jan 89 Ontario Environmental Network, 456 Spadina Ave.: In addition to the backup tapes referred to yesterday, there were about 300 floppies and a few PC's removed as well. Curiously, the most valuable PC in the room was untouched; it, however, had no data on its hard disk. The others, which did, were the ones taken.
- 17-19 Feb 89 Canadian Environmental Law Association, 243 Queen St. West: A computer and a small amount of cash was stolen.
- 6 Mar 89 Office of Hon. Jim Fulton, MP, Houses of Parliament, Ottawa: File on alleged open-air testing of chemical weapons at CFB Suffield in Alberta was rifled, contents possibly photocopied (Fulton keeps a high-speed photocopier in his office). Fulton says on 3 previous occasions he had noticed "evidence of break-ins," but had simply attributed the disorder to cleaning staff or new staff members. Two days after this break-in, Dr. Celso Mendoza, a specialist in biomedical defense employed in monitoring safety standards at CFB Suffield, was grilled for several hours by DND officials in a motel room in Medicine Hat, Alta. According to Mendoza, he was accused of "leaking politically embarrassing information to members of Parliament." In addition, a report has been circulated amongst Mendoza's colleagues accusing him of professional incompetence. Mendoza is preparing to sue the federal government over what he calls "constant harassment" by the DND.
- 10 April 89 Green Party of Canada, Vancouver office: Disks holding membership lists were stolen. No other equipment, including a stereo and a photocopier, was touched.

Yesterday Canadian Solicitor-General Pierre Blais, having previously claimed there was no link between the break-ins, said that he would order RCMP Commissioner Norman Inkster (who has also denied a link) to investigate the possibility of one. Blais also said he would speak to the minister for

National Defense, Bill McKnight, about the questioning of Dr. Mendoza. "These are serious allegations made by Mr. Fulton," said Blais. "They are already in the press and it's a very serious matter."

Said Fulton: "If five branches of the Toronto-Dominion Bank had been mugged in the last couple of months with the same kind of modus operandi, the same kind of files being rifled, ... there would be a major investigation going on. The names and addresses of tens of thousands of Canadians have been taken in these break-ins."

All of the thefts remain unsolved. According to Sergeant Len Paris of the University of Toronto police force, "Thefts of items under \$1000 don't attract a lot of police attention."

Hugh Miller, University of Toronto

## Computer orders for phone books (Only 17?)

Mark Brader <msb@sq.sq.com> Thu, 20 Apr 89 20:57:24 EDT

Today's Toronto Star has an article about a person who's been getting 17 telephone books delivered to his house each year for the past 5 years. The computer's role in this should be obvious. And I suppose it's not for the delivery people to say how many directories should be delivered to a particular place, just because it looks like a residence...

The Star says the victim says Bell Canada says he's actually supposed to be getting \*22\* phone books.

The directory has 2,084 pages and extra copies cost \$20 (Canadian). [each?]

Mark Brader, Toronto

### ATM's used to track accused killer

<forags@violet.berkeley.edu>
Mon, 24 Apr 89 10:03:32 PDT

According to a recent article in the Marin Independent-Journal, authorities were monitoring ATM transactions to trace the movements of accused killer Ramon Salcido. In addition to simply monitoring ATM use, his line of credit was changed to "unlimited" since authorities were afraid that he might become violent if he couldn't get money because he had exceeded his limit.

Al Stangenberger, Dept. of Forestry & Resource Mgt., 145 Mulford Hall, Univ. of Calif., Berkeley, CA 94720 (415) 642-4424

[In times of emergency such as this, we suspect that such requests can be legally by appropriate agencies without too much fuss. The question of course remains as to the extent to which your ATM and credit/debit

transactions remain private otherwise. The recent considerations for expanding the National Crime Information Center (discussed here in RISKS-8.27) rejected inclusion of such data from being routinely accessible to law enforcement officers... However, the fact that access is already so widely possible suggests that privacy is not easily enforced. PGN]

### Computer Voting (RISKS 8.60)

Chris Davis <smghy6c@buacca.bu.edu> Fri, 21 Apr 89 3:19:10 EDT

Boston U. has been using computers (Macs) to tally votes both this year and last. Many of the issues you mentioned have been, if not completely dealt with, at least started on:

The vote tally program is written in HyperCard. The keyboard (which is used to enter college and residence information for the non-University wide positions) is kept by the computer's owner (who is an official member of the student election process at that point). The mouse is used to check off votes, and when the user is finished, they leave. With only a mouse (and a limited number of buttons to use) it's hard to do much to the system by way of changing votes or crashing it... and privacy is kept by having the screen turned AWAY from the computer's owner while voting. There are, however, still some RISKS involved.

First is that of disk crashes. This happened this year--a certain number of votes were unreadable. (The student newspaper didn't give details, so I can't report on those.) They were not enough to have affected the Student Union race, though it's possible that they might have changed some college or residence races (no, I don't know for certain). An unscrupulous programmer may very well change votes, or the computer's owner could pull something (if they're technically capable--which isn't much with HyperCard).

The second is the RISK to the Mac user interface standard posed by the untrained (at least in Apple's guidelines) programmer. Not that this is a major RISK on the order of 767 fuel gauges, but it had a tendency to confuse me--precisely BECAUSE I use a Macintosh so often.

Chris "Data" Davis, Student Consultant, Boston University

#### Re: Most Accurate Clock

David Schachter <david%daisy@sri-unix.UUCP> Sat, 22 Apr 89 11:35:21 PST

In <u>Risks 8.58</u>, an article noted problems with assuming the correctness of time output by radio controlled clocks. I've a couple of notes on the subject and I speak as a designer of one such clock, Precision Standard Time's "Time Source".

1. The operator at WWV has been known to forget to set or reset the Daylight Savings Time switch on the time code generator in Colorado. We discovered

this because we were looking at the transmitted signal the day DST was supposed to start. When we received Hawaii (WWVH), the bit was set and when we received Colorado (WWV), it wasn't. We called WWV and asked what the problem was; they were rather abashed.

To solve this, PSTI is building new time code generators for WWV which will automate almost the entire task. Human intervention will be required to set the start and stop dates for DST, and to notify the time code generator of pending leap seconds, and the (very simple) software will take it from there. The design of the new time code generators, in both hardware and software, is intended to be very simple, so we can have a hope of correctness. This, of course, assumes the microprocessor and other VLSI chips we are using are, in fact, correct. Naturally, the hardware is triply-redundant. The software, however, is not, so common-mode failures will not be prevented.

2. Radio clocks are not perfect. Even if the software is bug-free, and the hardware is glitch-free (neither of which hold in practice), two major holes still exist: WWV, WWVH, WWVB, and, I believe, GOES, have no error detection or correction capability. It is possible for a radio clock to receive false radio data due to noise. In the PSTI clock, I put in a sophisticated algorithm to try and reject false data, but it is probabilistic: there is a chance the clock will output the wrong time. Most likely, an incorrect output will be wildly wrong, so host systems can reject it as bogus, reset the clock (or let it correct itself when "good" data overpowers the "bad"), and continue. Furthermore, if you are using a radio clock as a security measure, you should be aware how easy it is to falsify WWV, WWVH, and WWVB. For testing the PSTI clock, we built a WWV simulator, using the guts of another clock, and three 555-based oscillators. Hooking this into the modulation input of our venerable, WW-II vintage signal generator, we were able to create radio signals just like, but more powerful than, WWV and WWVH, and thence to fool the clock. This was great for testing, so we could check behavior of DST start/stop, propagation delay changes, year rollover, leap second insertion/deletion, and so on. But if you are using a radio clock for security, be warned that someone in a van outside your building can trivially fake the signal.

I bet the GPS satellite time signals contain error detection codes, if not error correction, which ought to reduce false time output to a minimum, but won't stop a bad person from faking the time.

Unfortunately, I couldn't get anyone interested in modifying the WWV/WWVH code to include a public-key encipherment approach, so that if the clock can decode the signal, the signal must have come from WWV/WWVH.

-- David Schachter

### ✓ Writing on write-protected 5.25" disks

"Leigh L. Klotz" <KLOTZ@AI.AI.MIT.EDU> Fri, 21 Apr 89 01:50:35 EDT

No software hackery is necessary. Simply open up the disk drive and tape the switch closed or put something opaque in the path of the light sensor. I once had to do this to fix defective software on some commercially duplicated disks

at a small software company.

## ✓ Re: Writing on "write protected" disks

Kenneth R. van Wyk <luken@ubu.cc.lehigh.edu> Fri, 21 Apr 89 09:27:23 EDT

In <u>Risks 8.61</u>, David M. Zielke and Peter Jones point out vulnerabilities of current write protect mechanisms. Specifically, they say that write protection is done at a software level on some microcomputers, including Apple IIs and (at least some) IBM PCs.

There was a heavily debated discussion on PC write protection mechanisms on the VIRUS-L forum not too long ago. The outcome was this: I looked at the IBM ROM listing and saw that the ROM was attempting a write (via the hardware disk drive controller) and \*then\* checking to see if there was an error status returned. Furthermore, two of our students, Richard Baum and John Hunt, checked the circuit diagrams of the original IBM PC floppy disk drives and determined that, indeed, the write protection mechanism was in hardware. Now, assuming that the write protect sensor is correctly determining the presence of a write protect tab, we concluded that no disk writes could occur.

It may or may not be different on other PC models (such as the AT that David Zielke refers to), but the IBM PC floppy disk write protection is done in hardware. I invite anyone to prove otherwise by providing me (or Risks) with a piece of code that can verifyably write to a write protected PC disk on a machine whose write protect mechanism is functioning.

Kenneth R. van Wyk, VIRUS-L moderator <luken@ubu.cc.lehigh.edu> or <luken@lehiibm1.bitnet>

[Readers who have been exposed to this in VIRUS-L or who don't care about PCs, clones, and Apples MAY IGNORE THE REST of this RISKS issue. Otherwise, please pardon the redundancy, although the following messages add a little bit here and there. But I'll blow the whistle after this issue. PGN]

### Apple write-protection

Omniphobe << PGOETZ@LOYVAX.BITNET<> Mon, 24 Apr 89 11:46 EST

Recently, a posting appeared in RISKS which claimed that the Apple write-protection is implemented in software. Wrong. Take it from me; I unfortunately know everything about the Apple ][+. Write-protection is implemented in hardware. Software routines are used to \_detect\_ write-protection. You can remove these routines and fool the operating system into thinking that it has written to a write-protected disk, but it has not. (In fact, I have performed this test under DOS 3.3 with a 5.25" drive.) It is possible that 3.5" drives might not have write-protection, just a tab detector, but I doubt it. It costs almost nothing to do it in hardware. I attribute the claim that IBM drives do not implement it in hardware to the

fact that the IBM is a shoddy conservative machine which can't even scroll the screen without flashing, and whose designers cannot compare to the Woz (who also designed the ][ 5.25" drive). But then, nobody can.

Apple drives sometimes destroy write-protected disks, but those cases are due to hardware problems.

Phil Goetz PGOETZ@LOYVAX.bitnet

### ✓ IBM PC's write protection is in the hardware!!!

<DLV%CUNYVMS1.BITNET@CUNYVM.CUNY.EDU>
Sat, 22 Apr 89 23:21 EST

Here is the reply to Mr. Zielke's letter that I sent to the IBM PC list. Since you chose to post his (uninformed) message, I think it would be a good idea to post my reply as well to aleviate some of the (totally baseless) fear and anxiety it might generate.

The technical reference to the Real IBM AT ('Personal computer AT high Capacity Diskette Drive', Aug. 31, 1984, pp. 7&8) clearly shows that the drive won't write unless the write protect sensor sees a hole. The protection is not in the software (DOS or BIOS) and not in the FDC firmware. It is done in the drive's hardware. If you want to write to disks with no notch in them, you have to disable the write protect sensor---a minor operation, but more than just writing some code. It requires a screwdriver. I suggest that you confirm this with your friend.

There was a long discussion in the virus list about whether the write protection on IBM PC is hardware or software; you may want to dig up its archive to read the sometimes heated discussion (Mac users stating that they know nothing about PCs but someone told them that only DOS calls check for write protection and BIOS calls will write irrespective of the notch; cheapo non-IBM drives that ignore black and/or mirror tabs; etc).

The question was settled for good in virus-I, and I hope there's no need for every un/misinformed user to submit his 2 bits worth to RISKS.

Dimitri Vulis, Department of Mathematics, CUNY Graduate Center

### ✓ Re: Writing on "write-protected" disks

<henry@utzoo.UUCP>
Fri, 21 Apr 89 23:24:14 -0400

>... Do RISKS

>readers know of other systems that are not protected at the hardware level?

It depends on what you mean by "at the hardware level". Almost any system with multiple heads (this includes most modern disk and tape) will find it difficult to run the final write signal to the heads via the write-protect switch. Any

other scheme introduces electronics between the switch and the heads, and those electronics can fail. Also, said electronics may well include firmware in microcontroller chips -- is this "hardware" protection? That aside, everything I'm familiar with does the write-protect check at a level where user programming can't affect it... but what horrors microcomputer companies will perpetrate to save a few cents, only they and their customers can tell. (As witness the original IBM PC monochrome monitor, which software could burn out by setting control registers improperly -- IBM borrowed the monitor from an earlier product which wasn't user-programmable.)

Henry Spencer at U of Toronto Zoology

# ★ Re: Writing on "write-protected" disks

<Kemp@DOCKMASTER.NCSC.MIL>
Fri, 21 Apr 89 23:37 EDT

I do not know what sort of Apple-]['s are used in Montreal, but mine certainly does have disk write protection in both hardware and software. Back in the days when Apple published schematics (before they made Macintoshes), their DOS manual contained schematics of both the disk controller card and the disk drive analog board. The analog board sits inside the disk drive and controls, among other things, the voltage applied to the erase head. The schematic shows that the write protect signal from the switch that senses the notch in the diskette is used to gate the write request signal from the controller, thus providing (in the absence of hardware failure) a non-overrideable write inhibit. The write protect signal was also provided to the controller card, where the software could query the write protect status of the drive.

Of course, many Apple owners were not afraid of modifying their hardware, and one particularly popular modification was to install an external write enable switch that bypassed the notch switch, or to disable the write protection entirely. This saved the user from having to cut notches in order to use the reverse side of single-sided diskettes.

Dave Kemp < Kemp@dockmaster.ncsc.mil>

### Re: Writing on "write protected" disks

Rich Sims <rich@pro-exchange.cts.com> Fri, 21 Apr 89 18:51:53 EDT

In digest #8.61 it is reported that it is possible for software to defeat the "write protection" notch on 5.25" disks, on both Apple and IBM disk drives.

I can not speak for all disk drive manufacturers, but in the case of the Apple drives, the information reported in the article is totally incorrect. Apple 5.25" disk drives use an electro-mechanical switch that prevents writing to the disk unless the "write protect" notch is unobstructed.

It is possible to defeat the software "sensing" of the write-protect switch,

but it is not possible to defeat the switch itself from software. If this is done, the only effect will be that the appropriate error message will not be presented to the user. The drive still can not write to the disk. Depending on how the software changes were made, there still may be an error message generated, when the O/S is unable to "verify" the supposedly written data.

It is still possible to destroy a disk though, given the right combination of hardware failures. In that case, the procedure recommended by the users group would be perfectly valid, and a very good idea. After all, if the hardware has failed to the extent of destroying disks, it makes good sense to test it on disks that you can afford to lose -- not your only copy of that \$500 program that helps keep your business running.

Of course, a competent hardware person can just .....: :-)

**Rich Sims** 



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 8: Issue 63

**Tuesday 25 April 1989** 

## Contents

- More 737 Computer Problems
  - **Brian Randell**
- Cockpit Computers Defy Pilots
  - **Robert Dorsett**
- Common thread in recent postings: People lan
- Smoke vs. disc drives
  - John Shipman
- Use of "Standard" on sensitive applications
  - Terry S. Arnold
- Computer Threat Research Association (UK)
  - David J. Ferbrache
- ATMs used to track accused killer
  - Steve Bellovin
- Re: Most Accurate Clock
  - **Don Watrous**
- Info on RISKS (comp.risks)

### ✓ More 737 Computer Problems

Brian Randell <Brian.Randell@newcastle.ac.uk> Tue, 25 Apr 89 10:33:26 BST

[This is a remailing of a hitherto undelivered 10 April posting from Brian Randell, Computing Laboratory, University of Newcastle upon Tyne.]

BOEING 737 PROBLEMS REACH FRESH HEIGHTS by John Kavanagh, Computer Weekly, 6 April 1989

Autopilot computer systems on Boeing 737s have been hit by a problem which has caused aircraft to change height without warning. It is believed that full details of the problem have been requested by the investigators into the crash of the British Midland 737 on the M1 motorway in January. One theory is that the crew were misled by cockpit instruments.

Six incidents have been recorded by British Airways on its aircraft but the company says there has never been any danger because the crews have always checked the autopilot actions against other cockpit instruments.

Boeing and Honeywell Avionics, manufacturer of the autopilot system, have alerted airlines using the 540-plus aircraft affected. "We have been working with the airlines and the regulatory autthorities to fix the problem." Boeing says.

The problem occurs after a pilot enters a new height to the autopilot. The system displays the instruction, but under certain circumstances the aircraft moves to a different height and the autopilot then displays the new reading.

One senior British Airways captain says the autopilot seems to use instructions entered earlier, even as long ago as the previous flight.

British Airways has called the problem "random memory initiation" and says it is caused by unexpected electromagnetic conditions such as lightning, strong radar signals, or an electrical power surge. Boeing says it has no evidence of any accidents occurring because of the problems.

### Cockpit Computers Defy Pilots

Robert Dorsett <mentat@dewey.cc.utexas.edu> Tue, 25 Apr 89 12:17:21 CDT

Cockpit Computers Defy Pilots
By David Learmount, Air Transport Editor
(From Flight International, 4/8/89)

Airliners have levelled out at incorrect flight levels as a result of flight management computers overriding pilot instructions. This results from a phenomenon which British Airways has named random memory initialisation (RMI). BA says that modifications it has carried out have eliminated the problem.

A line pilot has described RMI as "an increasingly common defect," although replacement of the microchips thought to be responsible is being carried out. The faults are most common, according to aircrew, in the early part ofa flight after the aircraft has been on the ground for some time. BA has experienced problems on all of its aircraft types fitted with electronic flight management systems.

The theory is that chips are retaining instructions which should have been overridden by the pilots' latest entry into the flight management system. The earlier instructions sometimes override the current ones, changing not only aircraft performance, but the digital display showing the effective instruction.

If the pilots are monitoring their flight management control display, they should see the change take place, or the incorrect entry come up. In busy phases of flight, however, such events have been missed.

A change in selected parameter has been known to tkae place in the 737-300. In the glass-cockpit 757 and 767, the more likely error is that the aircraft may fly through the set "height-acquire" flight level, or depart from the one it is at, although the value in the "height-acquire" window remains as selected. The latter two events are likely to be discovered quickly beacuse the crew will be monitoring flight level.

An airline pilot tells FLIGHT that some aircrew believe this sort of event may be contributing to pilots' scepticism about information displayed in modern cockpits—a human factor under investigation in the British Midlands 737 accident. Pilots may enter one set of of information, then act on different data which is displayed.

In one incident, a BA 737-300 on airtest out of Heathrow was cleared to descend to flight level 80 [8,000 feet]. The crew believe they entered FL80 in height-acquire, and saw it on the mode control display. The aircraft levelled at FL70, and air traffic control queried the action. The crew saw that FL70 was entered on the "height acquire" window of the flight management mode control panel and queried the ATC instruction. The pilot then set FL80 on "height-acquire" and climbed to it. The crew then flew level for a short time at FL80 and, while watching, saw the height-acquire display change to FL70.

Another 737-300 pilot has remarked to FLIGHT that, while dialling the height-acquire instruction, care is necessary because the display can settle one flight level above or below the figure entered.

BA admits to changes of these types occurring a recorded six times for a reason classified as "transient electromagnetic condition" (TMC), which they say has now been cleared by modification. TMC can be induced by current surges, and it is a well-known electronic phenomenon. Power surges or other forms of TMC can occur under well-recognised conditions, such as changeover from ground power supply to aircraft generators, lightning strikes, and radar proximity. Effects have also occurred when the cause was not obvious. It is not clear whether BA references to events resulting from TMC are the same--or related to--pilot reports of RMI detailed in BA's monthly Air Safety Review.

TMC problems have been dealt with by changes to software, hardware, and the mode select panel. BA says that there have been no further reports of problems since the modifications were made.

-----

#### An observation:

Modern glass cockpits (i.e., not the 757, 767, or A310) all use tape altimeters. Reading errors are common on such displays. In addition, these displays are not standardised; some scroll down to indicate increasing altitude; some scroll up. Some have a "highlight" window, showing current digital altitude; some don't. Setting errors, combined with read errors, could be fatal.

Media observation: pilots are being increasingly portrayed as "reactionary old fogies whose fears might actually be justified"--as if the manufacturers and the industry, in general, are the bearers of Light and Goodness. :-)

Robert Dorsett

Internet: mentat@walt.cc.utexas.edu

UUCP: ...cs.utexas.edu!walt.cc.utexas.edu!mentat

### Common thread in recent postings: People

<ian@lassen.sgi.com> Thu, 06 Apr 89 10:04:47 PDT

Many of the recent postings seem to have a lot in common. They all deal with some form of technological defect. Airbus accidents blamed on faulty computers, Audi 5000's effected by radio interferance, Elevators in which Micro processors fail to detect open or blocked doors, fire control systems which mis-identify civilian planes, the list goes on.

Each of the incidents above have, of course, another thing in common, they were designed by humans.

What are the risks associated with technology we don't properly understand? As we have modernized elevators, planes, cars and fire control systems, they seem to have become not only more complicated but more trouble prone.

I am reminded that K(eep) I(t) S(imple) S(tupid) is perhaps something we should reevalute by the NOVA episode "Beyond Top Gun" in which Korean war pilots said, while flying in Vietnam, the first thing they did in a dogfight was start turning things off starting with the back seaters' intercomm followed by some of the warning buzzers and other techno whiz bangs.

lan

### Smoke vs. disc drives

John Shipman <john@jupiter.nmt.edu> Sat, 22 Apr 89 13:40:09 MDT

One advantage of Winchester-type disc drives is that they are sealed against smoke and other particulates. Hard drives with removable media, however, must have ``absolute'' filters, since smoke particles are larger than the flying height of a typical disc head. It's a fine theory to warn your customers not to smoke, but who's going to check up on third-shift operators?

At a famous West Coast computer company where I worked in the early seventies, the newly founded disc division had just shipped their first production drive to the computer division for testing. A friend of mine in Systems Integration believed it was not his duty to coddle the equipment, but to subject it to more typical real-world conditions. He installed the drive, got the diagnostics running on it, and then lit a cigar and proceeded to exhale all the smoke directly into the disc's air intake. SPANG---head crash.

The disc division tried to "blame the messenger" and wanted my friend fired, but the computer division backed him up. Result: by

the time this model went to real customers, it had an absolute filtration system, and eventually proved to be quite reliable.

### ✓ Use of "Standard" on sensitive applications

"Terry S. Arnold" <Arnold@DOCKMASTER.ARPA> Mon, 24 Apr 89 22:49 EDT

What do the readers of this forum think are the risks involved in using "Standard" tools such as lex or yacc etc. in developing sensitive applications? Is it reasonable to set some criteriaa for saying that a given tool has withstood the test of time therefore it can be safely used? If so what should this criteria be?

Terry Arnold

## Computer Threat Research Association (UK)

"David.J.Ferbrache" <davidf@cs.heriot-watt.ac.uk> 31 Mar 89 09:03:40 GMT

For those of you interested an umbrella organisation has been established in the UK to co-ordinate information on, and research into, all aspects of computer security. In the first instance one of the organisation's primary concerns will be combatting the threat posed by computer viruses by acting as a clearing house for virus information and control software.

Below is a copy of an initial letter mailed to prospective members:

The Computer Threat Research Association

The computer threat research association, CoTra is a non-profit making organisation that exists to research, analyse, publicise and find solutions for threats to the integrity and reliability of computer systems.

The issue that caused the formation of CoTra was the rise of the computer virus. This problem has since become surrounded by fear, uncertainty and doubt. To the average user the computer virus and its implications are a worry of an unknown scale. To a few unfortunates whose systems have become a critical issue.

The key advantage of CoTra membership will be access to advice and information. Advice will be provided through publications, an electronic conference (a closed conference for CoTra's members has been created on the Compulink CIX system) as well as other channels such as general postings direct to members when a new virus is discovered.

CoTra membership will be available on a student, full or corporate member basis. All software that is held by CoTra that enhances system reliability, such as virus detection and removal software, will be available to all members. It is intended to establish discounts with suppliers of reliability tools and services. A library of virus sources and executables and other

dangerous research material will be made available to members who have a demonstrable need.

A register of consultants who have specific skills in the systems reliability field will be published by CoTra and reviews of reliability enhancing software will be produced.

Your support of CoTra will ensure that you have the earliest and most accurate information about potential threats to your computer systems.

CoTra, The computer threat research association, c/o 144 Sheerstock, Haddenham, Bucks. HP17 8EX

-----

Part of the organisations aims is to establish reciprocal links with other similar organisations worldwide, to facilitate the sharing of experience and rapid flow of information on new threats.

To this end if you are involved in (or have contacts with) a similar organisation in your country, please write to CoTra (or by email to me, and I will forward your correspondence) outlining your organisation and its aims.

Yours sincerely

Dave Ferbrache Personal mail to:

Dept of computer science Internet <davidf@cs.hw.ac.uk>
Heriot-Watt University Janet <davidf@uk.ac.hw.cs>
79 Grassmarket UUCP ..!mcvax!hwcs!davidf

Edinburgh, UK. EH1 2HJ Tel (UK) 031-225-6465 ext 553

## ✓ ATMs used to track accused killer

<smb@arpa.att.com>
Tue, 25 Apr 89 08:02:19 EDT

In times of emergency such as this, we suspect that such requests can be [used] legally by appropriate agencies without too much fuss.

Part of the problem here is not that the technique was used, but that it was done without judicial approval. The bank \*chose\* to co-operate, on the word of the police authorities. In this case, the situation was fairly clear. What if it's a foreign student who is accused of being a ``terrorist''? Such accusations by the government have already been thrown out of court on several occasions. (The student may or may not be one; that's irrelevant.)

--Steve Bellovin

✓ Re: Most Accurate Clock (RISKS 8.62)

<watrous@aramis.rutgers.edu>
Tue, 25 Apr 89 10:04:33 EDT

- > Date: Sat, 22 Apr 89 11:35:21 PST
- > From: David Schachter <david%daisy@sri-unix.UUCP>
- > Unfortunately, I couldn't get anyone interested in modifying the
- > WWV/WWVH code to include a public-key encipherment approach, so that
- > if the clock can decode the signal, the signal must have come from WWV/WWVH.
- > -- David Schachter

The signal must have come from WWV/WWVH \_at some time\_! This would verify the source of the signal, but not the timeliness. Your clocks could be set back by broadcasting a tape of WWV/WWVH. The encipherment only solves half the problem.

Don



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 8: Issue 64

# Wednesday 26 April 1989

### Contents

DARPA studying high-tech surveillance for drug wars

Jon Jacky

Re: SKYDOME

Michael Wagner

Cursing the Darkness?

Ronald J Bottomly

Data Checking at Osco's

**Scott Turner** 

Re: Common thread in recent postings: People

**Hugh Miller** 

John Karabaic

Re: Use of "Standard" ...

**Pete Schilling** 

Steve Bellovin

Info on RISKS (comp.risks)

### DARPA studying high-tech surveillance for drug wars

<JON.JACKY@GAFFER.RAD.WASHINGTON.EDU> 26 Apr 1989 09:05:20 EST

The following excerpts are from FEDERAL COMPUTER WEEK, vol 3 no 17, April 24 1989, pages 1, 53:

DARPA PROGRAM TO BATTLE WAR ON DRUGS, TERRORISM by Gary H. Anthes

The Defense Advanced Research Projects Agency is quietly putting together a multimillion-dollar program to develop advanced computer technology for the wars on drugs and terrorism.

The technology is likely to be built on a foundation of artificial intelligence and parallel processing, and it will be applied in situations that the Defense Department refers to as special operations/low intensity conflicts, or SO/LIC. The new program is headed by William Marquitz, deputy director of DARPA's Information Science and Technology Office and a veteran of the Central Intelligence Agency and the Pentagon's command, control, communications and intelligence unit.

According to Marquitz, much data that could be useful in counternarcotics and counterterrorism --- for tracking currency, cargo shipments and phone call patterns, for instance --- is readily available. But the government has generally has not brought to bear fast computers that can examine trillions of bits of information per day and smart software able to distill out the tiny amounts of useful information. ...

One agency with a small research budget is the Drug Enforcement Administration. According to Marquitz, DEA manually reviews printouts of international telephone calls, looking for suspicious patterns.

For example, repeated calls to South America from a private residence in Miami might trigger some sort of investigation.

Obviously such a procedure is tedious and error-prone. Marquitz envisions a fast parallel processor running an expert system that can examine millions of telephone calls a day and discern subtle and complex patterns for follow-up by law enforcement officials. Marquitz says it isn't a problem of data collection but of data fusion and reduction, a process he calls "digging the signal out of the noise".

Opportunities to marry AI, parallel processing and pattern recognition techniques exist in several other areas, Marquitz said. A great deal of cocaine enters the country in cargo containers that mysteriously disappear for days at a time and then magically reappear. ``The data to track these containers is available in manifest records and can be readily supplied, but it is not automated," Marquitz said. A computer system could track the movement of these boxes on a near real-time basis, looking for anomalous conditions, he said.

In another example, Marquitz said currency-tracking schemes could be devised, not for checks and credit card transactions, which drug distributors never use, but for greenbacks based on their serial numbers.

Marquitz said DARPA's current focus on counternarcotics has roots in the past. "During the [presidential] campaign, there was a lot of debate about drugs; the campaign highlighted the issue. We were already looking at the more general problem of SO/LIC, so we were up to speed about thinking about these problems. Now we are way out ahead," he said.

Marquitz also said DARPA officials are working on a five-year plan for research and prototype development in SO/LIC.

- Jonathan Jacky, University of Washington

★ Re: SKYDOME (Risks 8.62)

Michael Wagner <MICHAEL@vm.utcs.utoronto.ca> Wed, 26 Apr 89 16:05:54 EDT

> [This of course contradicts the myth that smaller programs run faster. PGN]

It also contradicts the story that I heard. One of my clients is an architect who lives 2 blocks away from the SKYDOME. Living next door, he is very interested in the SKYDOME (including the undercapacity transit plans, but that's better left to another RISKS submission), and being an architect, he hears many interesting things. According to him, the stress on the dome from opening and closing the dome was badly underestimated, and current estimates are only 4 times a year will be safe (down from an original projection in the 30-40 range), i.e. any more will dangerously stress the machinery and lead to early failure. I tried, without success, to determine what sort of assumptions this revised estimate was based on, but it's not his area of expertise, so he couldn't help me much.

From the little he told me, I can't determine whether a software rewrite would be capable of "solving" this problem or not.

Michael

### Cursing the Darkness?

Ronald J Bottomly <Bottomly@DOCKMASTER.NCSC.MIL> Wed, 26 Apr 89 15:20 EDT

I know this is usually reserved for computer risks, but I've discovered a heretofore-unknown (at least to me) advantage.

Last night my block experienced a power outage. And since my place is all-electric, I was left totally in the dark (without candles, flashlights, etc). The only self-contained light source that I could find was the eerie blue glow emitted from my lap-top computer.

As I wandered about like a computer-age Diogenes, I thought it ironic that the only thing to operate during a blackout was a computer.

## Data Checking at Osco's

<srt@aerospace.aero.org>
Wed, 26 Apr 89 13:09:10 -0700

As an example of "anti-risk" I was interested to observe during a recent shopping trip that the computerized registers at Osco's (a local drug store chain) query the cashier when a questionable price is entered, apparently according to the category of the item (which the cashier enters separately). In this case, the cashier had entered a price of \$79 for a skin care product, and the register politely inquired whether he had made a mistake (as, indeed, he had).

-- Scott Turner

### Re: Common thread in recent postings: People (RISKS-8.63)

Hugh Miller <MILLER@vm.epas.utoronto.ca> Wed, 26 Apr 89 09:49:47 EDT

The requirement that systems be kept simple is itself too simple to "manage" technology -- if, indeed, WE manage IT, and not the other way around. Nor is simplicity necessarily a virtue if a simplified tool magnifies its potential for control, control of events AND persons. Making a tool less "option-rich," even at the cost of decreased flexibility, is not the answer to our problem, because the problem it IS an answer to (how to smoothly adapt a control function to an irregular domain) is not the central one. The central problem is whether all this technology serves a good, "The Good" if you will. Crucial to that problem is the question of whether nature -- our own included -- can and should be adequately characterised as an "irregular domain" for the possible employment of technology.

That it does we take more or less for granted, at least at the policy-planning level. (Our consciences, we hold, are our "private" affair.) A recent posting in the alt.fusion newsgroup castigated the opinions of people like Paul Ehrlich and Jeremy Rifkin, who have questioned whether such a thing as a "Utah tokamak" cold-fusion reactor might not be bad for us after all. "What pieces of disgusting slime they are," wrote the author. "Fortunately, with something this important they will be ignored, and, if they interfere, steamrollered." I fear his attitude, more temperately phrased, is shared by the great majority of us.

Steven Kull, a psychoanalyst, interviewed a number of DoD, military, and defense-related industry types for his recent book \_Minds at War\_ (New York: Basic Books, 1988). His aim in the book was to examine the psychological attitudes of nuclear strategists. Especially interesting (and chilling) was an observation he made about interviews on the subject of the big push for hard-target kill capability (GPS, Navstar, earth-penetrating warheads, etc.). Those of us who work in similarly computer-intensive milieux would do well to adapt it to our own work:

A rather curious widespread attitude was that the United States "might as well" improve its hard-target capability given that it had the technological ability, as if the effort to improve such capabilities was virtually costless. Even respondents who understood and were actually sympathetic to concerns about the instabilities engendered by hard-target kill capability often shook their heads as if to say that only an overwhelming logical argument could stop such technological developments. There was a pervasive feeling that despite multibillion-dollar costs, building new weapons with greater accuracy was virtually effortless, while refraining from doing so was a gargantuan effort. Some simply asserted that the weapon in question was a good weapon in a technical sense and therefore should be built. In a few cases, respondents even seemed surprised when pushed for a stronger rationale based on strategic

considerations.

Hugh Miller, University of Toronto

### Re: Common thread in recent postings: People (RISKS-8.63)

John Karabaic <fuzzy@aruba.arpa> Wed, 26 Apr 89 12:14:43 EDT

[...] this brings up another RISK: the effect our organizations have on the use/misuse of technology. The problem I'll tell about was not a technological one, it was a bureacratic one, but if it had not been solved a technological RISK would have resulted.

I used to work in an Air Force Systems Command System Program Office as an Avionics Project Manager. One of the boxes I had responsibility for was the Intercom Set Control Panel (ICSCP), which controlled the radios, the pilot/weapon systems officer intercom, and voice warnings on one particular fighter. Voice warnings occurred for events like low fuel; a digitized female voice would say, "Bingo Fuel. Bingo Fuel." The warning would occur everytime that interrupt occurred, so if you were jigging the plane around to avoid getting killed, fuel slosh might generate many warnings.{\footnote The voice, on early versions of the aircraft, belonged to a woman from Florida known as "Bitchin' Betty". When we decided to redigitize for our aircraft, her voice quality had changed and "Caustic Kristen" took her place. Female voices are preferred because pilots (overwhelmingly male) react more quickly to them.}

Here's where the fun begins: the voice warnings attenuated all radio and intercom messages by 23dB. So let's say you're doing the aforementioned jigging: you could miss a critical radio transmission ("Number two, you're going to hit the ground", "Number three, you have a MIG on your tail") and die. This problem had been corrected on earlier versions of the aircraft by just removing the attenuation; the pilots could correctly distinguish and interpret two or three simultaneous messages. The requirements fellows had told my office to correct it for the new version. This got lost in the organizational cracks; I dug it up when I was going through old message traffic after I was given management of the program. The attenuation was embedded into an approved high-level, baseline specification and had trickled down into at least two lower-level specs. An engineering change proposal would have to be made if we followed the rule book.

We were well into full-scale development, and two or three preproduction ICSCP's had been made. The firmware was really firm; we would have to rip out the old chips (and fatigue the boards) and install new ones. The way the USAF does business, it takes two years before you can even have the contractor start work on an engineering change (it takes that long to jump through all the hoops). By that time, about forty systems would be in the field. We would have to retrofit each one at a cost of millions of dollars for the entire program. The change was not safety-critical; that had been determined when they changed the older versions of the aircraft, so we couldn't put out an "urgent" change. A safety-critical mod would not have looked good when our budget went before Congress, either.

So, what to do? I made a visit to the ICSCP subcontractor with my main contractor and we determined that we could either cut a single wire or make a two-line software change. Wire-cutting was a kludge I wanted to avoid, but it started looking awfully attractive: the USAF was not buying any software documentation, so we hadn't a clue about what to change if we wanted to modify the software organically and wire-cutting is something the intermediate shops could do. Remember that the contractors have little interest in actually making the change \*now\*: the baseline has been approved and they stand to make lots of money off the retrofit program if we go the software way (and maybe even if we cut the wire). But by some gentle convincing and appeals to professional pride (and the promise to tell the Advanced Tactical Fighter SPO what a great job they had done in averting a costly retrofit), I told them to make the change to the spec and modify the software and I would make sure the SPO would approve it. It was done, and the retrofit avoided. I called some friends at ATF and told them the whole story.

Lessons learned: The machinery we set up to manage our large projects carries RISKS of its own. If we had gone by the book, forty+ aircraft would have been in the field with a RISKy condition. By having a very professional contractor with a liberal dose of enlightened self interest, a problem with our organizational machinery was circumvented. I'm sure other organizations have had similar problems, and solved them in similar ways.

Lt John S. Karabaic, WRDC/TXI, WPAFB, OH 45433-6543 513 255 5800 These opinions are mine.

BTW, the operators (pilots and WSO's) hated the voice warnings with a vengeance. They much preferred simple tones and warning lights. But high-tech sells...

## ★ Re: Use of "Standard" on sensitive applications

"ALBTSB::SCHILLING1" <schilling1%albtsb.decnet@aldncf.alcoa.com> 26 Apr 89 15:12:00 EST

In fields that are mature enough to have liability associated with wrong actions, users of standard products have the protection of the law. Real standards exist for things like steel beams, so a designer or builder can order beams and expect that they will perform as specified in the standard. The standard specification for steel beams requires tests using standard methods which are understood and accepted by competent engineers, who use standard terminology in communicating with one another. If a beam fails in service, then the builder's lawyers call the beam maker's lawyers to discuss things like compensatory and punitive damages. The threat of liability for wrong action keeps most people honest enough to avoid lawsuits.

Real engineers would laugh at the idea that lex and yacc are "standard" products. What standard specification do they satisfy? What standard test methods verify that the particular version of lex or yacc used to develop a system conforms to the specification? What standard rules of design, developed by recognized groups of experienced professionals, guide other competent professionals as to how lex and yacc should be

used? What standard defines the terms in which competent professionals communicate about these tools? Who do a system builder's lawyers talk with if the tools fail in service?

Pete Schilling, Applied Mathematics and Computer Technology Divn., Aluminum Co. of America, Alcoa Center, PA 15069 Alcoa Laboratories 412/337-2724

## ✓ Use of "Standard" on sensitive applications

<smb@arpa.att.com>
Tue, 25 Apr 89 23:53:28 EDT

I don't think there's an absolute rule here; a lot depends on the application and its history. For a task that's very well understood theoretically -- i.e., parsing or lexical analysis -- a good tool is likely to be far more reliable than a hand-coded equivalent, and far more consistent besides. A similar rule can be applied to very complex tasks, such as protocol design; if your primary goal isn't (for example) to design a new transport protocol, you're much better off using a standard one. The bugs are often subtle, and today's protocols are the product of years of experience.

It's the middle range where I'm more skeptical; one needs reason to trust something. If an application is complex, an existing tool often doesn't quite fit; adding just a few little hacks is a sure road to disaster. We often see this in newspaper horror stories about municipal accounting systems that are years late and millions over budget -- even though the general concept is straight-forward enough, all the little special cases can kill the project.

--Steve Bellovin



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 8: Issue 65

# Thursday 27 April 1989

### Contents

- Northwest 255 -- Another Disconnected Alarm story? Jerry Leichter
- All addressed up with the wrong place to go Jerry Leichter
- Jukebox foolishness Robert J. Reschly Jr.
- Electronic Seat-Belts
  - Marc W. Mengel
- Mitnick plea bargain rejected by judge as too lenient **Rodney Hoffman**
- Spider-Man's SSN and computer limitations **Brad Blumenthal**
- Info on RISKS (comp.risks)

### Northwest 255 -- Another Disconnected Alarm story?

LEICHTER-JERRY@CS.YALE.EDU <"Jerry Leichter> Wed, 26 Apr 89 20:51 EDT

From the New Haven Register, 24 Apr 89. (Page 30)

Pilots in Northwest crash accused of disconnecting alarm on another flight

(Associated Press) Detroit: There is evidence that the pilots involved in a deadly 1987 airliner crash, blamed in part on a warning system failure, intentionally disconnected a similar alarm on another jet two days earlier, the plane's maker says.

In a petition filed with the National Transportation Safety Board, Douglas Aircraft Co., a division of McDonnell Douglas Corp., said the pilots pulled a warning system circuit breaker on the first plane, interrupting power to the system and silencing an unwanted warning, The Detroit News reported Sunday. The same pilots, John Maus and David Dodds, were in control of Northwest Flight 255, a McDonnell Douglas MD-80, when it crashed on takeoff at Detroit Metropolitan Airport on Aug. 16, 1987.

The pilots died, along with 154 other people, including two people on the ground. The only survivor from the plane was a 4-year-old girl. It was the second worst aircraft accidednt in U.S. history behind the 1979 crash of an American Airlines jet near Chicago that killed 275 people.

The NTSB concluded last May that the warning system on the MD-80 failed to alert the pilots that they hadn't set the wing flaps and slats, which provide added lift for takeoff.

The board faulted the pilots for not setting the flaps and slats and failing to complete a routine pre-flight checklist. The board also said power to the warning system was interrupted, but couldn't determine why.

Douglas' petition, obtained by the newpaper, cited a note written by Northwest pilot Merrill Hodges in September 1987. Hodges said he found an alarm system circuit breaker pulled on another MD-80 jet flown by Maus and Dodds.

Flight records show Maus and Dodds landed that plane in Santa Anna, Calif., on Aug. 14, 1987, and the plane stayed on the ground until Hodges entered the cockpit the next day, Douglas' petition said.

"The unavoidable conclusion is that the absence of power to the takeoff warning system was the flight crew's intentional disablement of the takeoff warning," the petition said.

Northwest lawyer Carroll Dubuc said Douglas' petition doesn't raise anything new and promised to file a response that will rebut Douglas' claim.

The newspaper quoted an unidentified official of the Air Line Pilots Association as saying the claim is false. The official said the union is also preparing a response.

# All addressed up with the wrong place to go

LEICHTER-JERRY@CS.YALE.EDU <"Jerry Leichter> Wed, 26 Apr 89 21:14 EDT

[Background: Martindale and Hubbell is, and has been for many years, the standard directory of lawyers and law offices. It runs to many thick volumes, and is a required part of any law library.]

From "The American Lawyer", April 1989. (Page 19.)

If you want to serve process on New York's Weil, Gotshal & Manges, you could be handing papers to a dapper, red-liveried doorman at The Belmont, an exclusive residential building on Manhattan's East 46th Street. Mail addressed to Whitman & Ransom could end up in the hands of one J. Pugh, the tenant in apartment 5A of The Vancortlandt, a tony upper Park Avenue building. And

lawyers unfamiliar with Wall Street's Fried, Frank, Harris, Shriver & Jacobson could be reporting to a luxury apartment building on the Upper East Side.

Although the Belmont's doorman doesn't work for Weil, Gotshal, he says he has been receiving "all kinds of mail" for the firm. "Maybe a few lawyers live in this building," he adds, "but there is no law firm here."

It seems that Martindale-Hubbell, Inc., made a few mistakes in printing its 1989 New York law directory. Twelve New York firms - including Weil, Gotshal; Fried, Frank; Whitman & Ransom; Phillips, Nizer, Benjamin, Krim & Ballon; and Kelley Drye & Warren - are listed with incorrect, and seemingly random, Manhattan addresses.

"I'm not very happy with [Martindale]," says Weil, Gotshal partner Alan Weinschel. "This is the most god-awful negligence. Suppose somebody serves papers on us at [East 46th Street] and it takes an extra day to forward it to our office [at 767 Fifth Avenue]? What if we miss a deadline because somebody didn't make a change in the directory?"

Martindale cannot explain the erroneous addresses, except to blame "a computer glitch," according to Richard Pizzi, vice-president and corporate counsel to the legal publishing company. Pizzi says the company's computer was "turned down, and then back up" after the New York volume was already proofread. Martindale didn't discover the errors until after the volume was printed and mailed.

"We tried to address the issue head on," Pizzi says, noting that the company gave each affected firm a complete refund of the cost of printing attorney's biographies in the volume. The publisher also arranged with the post office for mail to be forwarded to the proper addresses, and sent customers a two-page announcement of corrections. Nonetheless one firm is sending a messenger four times a day to pick up Federal Express mail and other deliveries that might have found their way to the incorrect address.

Martindale's efforts haven't earned high marks from some lawyers at the affected firms. One angry partner says that when he insisted Martindale issue stick-on labels with the correct addresses, the company didn't respond. (Prizzi says the company is considering the suggestion.) Pizzi turned down requests from firms who wanted the book reprinted.

But other firms involved in the mix-up are not concerned. The Manhattan branch of Rochester's Nixon, Hargrave, Devans & Doyle, for example, is listed at two addresses - 30 Rockefeller Center, its true address, and 101 Park Avenue. "Our regular customers know where we are," says Edward Hughes, managing partner of the New York office. "We'll rely on everybody's good humor to get by." ----Karen Dillon

### Jukebox foolishness

"Robert J. Reschly Jr." <reschly@BRL.MIL> Thu, 27 Apr 89 4:14:22 EDT Here is yet another example of microprocessor programming foolishness: When several of us went to the local Pizza Slut for supper this evening, we were seated next to the jukebox. After noting that it looked pretty new we proceeded to forget about it until it went into "attract mode".

If it remains unused, it will eventually play a seemingly randomly chosen song about once every 15 minutes. This behavior, a relatively trivial extension of the attract mode common to video games, did not elicit much comment. It did however provoke more intense scrutiny of the jukebox. There were several 7-segment displays making up the front panel (the usual "current selection", "current play", and so forth), and one labeled "most popular selection".

Given that the group was composed of techie types, we proceeded to speculate on the usefulness of that display -- including the idea of feeding the play history to a clearinghouse ala Arbitron or Nielson. We also started wondering if the people who programmed the jukebox remembered to exclude the selections played during attract mode from the "most popular selection" calculations.

Answer: NO! When the jukebox played "143" in attract mode, the "most popular selection" display switched from "165" to "143". \*Sigh\*

Bob

[I'm glad it wasn't a JOKEBOX. Nothing like hearing the same jokes over again, even if you tell 'em by the numbers. (Old metajoke) To go with "You didn't tell it very well." and "We never heard that one before.", how about these:

"Number 165? That's not funny anymore. The jokebox keeps playing it." "Number 143? I couldn't understand that one. It was still encrypted."

### Electronic Seat-Belts

Marc W. Mengel <mmengel@cuuxb.ATT.COM> 27 Apr 89 16:38:30 GMT

>From Automotive Electronics News, Monday April 24 1989, p31

Makers Ready Smart Seat Belts for Mid-'90s Entry

DETROIT - Seat belts with electronic tension and slack controls should be commonplace on cars in the 1990s, according to manufacturers. ... Research shows that the more comfortable belts are, the more likely people are to wear them. The problem is that belts are more comfortable when they exert less tension on the body, but they provide the most protection when they are snug. ... Common mechanical belts in US cars today control slack with ratchets and pawls similar to window shade mechanisms. ... Mechanical belts' major drawback is that sometimes too much slack is left in a belt when a person leans forward and then sits back in the seat.

A survey in 1988 by the Insurance Institute for Highway Safety showed that more than one-third of the belted drivers of American cars have greater than the safe limit of 1 inch of slack in their restraint. This phenomenon contributed to more severe head and facial injuries. ... Engineers at Bendix

Safety Restraints Division of Allied Signal Corp. and TRW Vehicle Safety Systems Inc. -- the two major seat belt suppliers said electronically controlled belts with electronic slack controls will provide maximum safety and maximum comfort.

Both companies have developed prototype belts with electronic slack controls and have presented them to their Big Three customers for evaluation. ... Once electronics are made part of a seat belt system, other features can be added easily, said Dr. Fleming [staff engineer in R&D at TRW] ... Sensing brake pressure is important because a driver whose car is sliding on ice might brake, and an inertial sensor might not pick it up, said Dr. Fleming. With electronics "It doesn't cost you anything to lock those belts ... and drive the motor backwards to really tighten down the belt," he said. This would be accomplished by having an algorithm that signals the seat belt motor to temporarily run in reverse at double voltage during an emergency situation, Dr. Fleming said. ... These smart systems might then lead to anticipatory systems that use radar as the sensor, ... Systems also can be created to adapt themselves to individual occupants tastes for slack and tension.

[What about electrical systems failures leading to loss of control \*and\* loss of seat belt locking??? Marc Mengel]

[How about "brilliant belts" that sense when you are drunk, strap you in, and call the police? PGN]

## Mitnick plea bargain rejected by judge as too lenient

Rodney Hoffman <Hoffman.ElSegundo@Xerox.com> 26 Apr 89 08:13:46 PDT (Wednesday)

An article by Kim Murphy in the 25 April 1989 'Los Angeles Times' reports that U.S. District Judge Mariana Pfaelzer unexpectedly rejected the plea bargain of Kevin Mitnick, the hacker once called "as dangerous with a keyboard as a bank robber with a gun." Pfaelzer declared that Mitnick deserves more time behind bars.

As reported in RISKS 8.43, "Mitnick pleaded guilty to one count of computer fraud and one count of possessing unauthorized long-distance telephone codes.... Mitnick faces one year in prison. Under a plea agreement with the government, he must also submit to three years' supervision by probation officers after his release from prison."

Judge Pfaelzer said Monday, "Mr. Mitnick , you have been engaging in this conduct for too long, and no one has actually punished you. This is the last time you are going to do this." She said a confidential pre-sentence report recommended that she exceed even the 18-month maximum prison term called for under mandatory new federal sentencing guidelines. The judge's action voids Mitnick's guilty plea.

Both prosecuting and defense attorneys were surprised. Mitnick's attorney said he did not know whether his client would agree to a guilty plea carrying a longer prison term. This could make it harder to bring charges against

Mitnick's alleged associates. If Mitnick is brought to trial, testimony from at least one of his associates would be required to convict him, and they would not appear as witnesses without receiving immunity from prosecution.

### Spider-Man's SSN and computer limitations

<brad@cs.utexas.edu>
Thu, 27 Apr 89 10:03:09 CDT

I guess we've probably beat this topic about to death, but comic strips do give some picture of popular beliefs about computers. The current story line in Spider-Man has Jolly Jonah attempting to discover the web-slinger's True Identity by hiring a team of psychologists to "feed information into a computer," which will then figure out the answer.

This is not the only time I've run across this sort of computer naivete. When I was just learning to program (in BASIC, lo these many years ago), a friend called me up with a scheme to win a local radio station contest. I would take all the clues that the station had broadcast describing, and "feed" them into "the computer" (presumably into the BASIC interpreter :-), and he would figure out some way to get through to the radio station when the computer came up with the right answer.

The question for RISKS readers is double-edged. How did this impression of computers as all-knowing come about, and how should we, as professionals, describe computers so as to dispel these notions? The answer to the first part of the question is fairly obvious. A friend pointed out to me the multitude of public sources of misconception -- from popular entertainment (Twilight Zone, 2001, Knight Rider), to sales campaigns and news reports based on press releases (users will be able to train themselves and solve world problems with computer X), to sensationalistic claims by well-known and highly visible computer scientists.

The other side of the question is much harder. I've often found myself trying to characterize the limitations of computers as they are applied to these situations (i.e. discovering an identity from a set of clues). It's an interesting juxtaposition to the awesome ability computers have for producing a set of clues from an identity (e.g. a SSN). Trying to explain the differences in cocktail-party English is difficult at best. As our data bases become larger the principle of garbage-in-garbage-out seems to be taken less seriously (ironically), and non-computerniks don't seem to interpret this to include nothing-in-nothing-out.

To reiterate, how should we present the limitations of computerized information handling in a clear, non-patronizing way, and how can we effectively counter those who imply the omniscience of "The Computer?" Do we need a "truth-in-advertising" code for computer capabilities; if so, what should it look like?

Brad Blumenthal, Computer Science Department, University of Texas, Austin TX uucp: {uunet, harvard}!cs.utexas.edu!brad



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 8: Issue 66

# Thursday 4 May 1989

## Contents

Standards == nothing

**Rich Neitzel** 

Traffic Alert Collision Avoidance System with "no bugs"

**Henry Schaffer** 

Nuclear reactor knocked offline by 2-way radio in control room

Wm. Randolph Franklin

B-2 builders: Prototype not needed (Long Article)

Mark Thompson via Stephen W. Thompson

American Express is watching...

Sundar Iyengar

Telephone line security

David C. Kovar

COMPASS Program

John Cherniavsky

Info on RISKS (comp.risks)

### Standards == nothing

Rich Neitzel <thor@stout.UCAR.EDU> Mon, 1 May 89 13:44:52 MDT

Before deciding that I enjoyed software development more then engineering, I was involved in nondestructive testing (NDT). One of the major functions of NDT is to determine the adherence of the item under test to standards. Generally these standards are related to the safety of the larger system in which the the tested item is a component. My experience directly contradicts that expounded above. Anyone who orders and uses a product simply based on its "meeting" standards is being extremely foolish.

For example, an NDT lab that I worked for was owned by a steel warehouse firm. The parent had a contract to supply structural steel for a major office complex. Twice the firm purchased steel only to discover that the mill certificates were faked. In the first case, this was discovered only when welders reported problems during fabrication. This kind of problem is more

widespread then most people would like to admit. Consider the recent spate of reports on substandard areospace fitting being sold with false documentation.

Further, I was several times asked to falsify NDT results to certify that items met standards. In one case, I failed a number of welders taking a certification examination (on the same building project noted above). The fabricator simply took the SAME weld coupons to another lab and EVERY ONE of the welders passed. In another case, at nuclear weapons plant I worked at, a team of EE's was prevented from inserting additional circuitry into a test system that would falsify test results only when one threatened to go public with the information.

While the above examples are concerned with outright fraud, many things involved in applying standards are open to interpretation. Consider the RS-232 standard. How does an inspector of power plant welds determine if an ultrasonic echo means the weld is substandard, when it is the "gray" zone? Many standard compliant items are not in compliance.

The point of all this is that standards guarantee little or nothing. Questions of liability are meaningless. If the profit to be made is high enough and the risk of detection small enough, many firms will falsify certification. Worse, the falsification may be impossible to trace. A part fails and loss occurrs, but often the damage is such that no reconstruction of the exact cause can be made. Since the part was certified, the search is likely to turn elsewhere (assembly, operation, etc.). I am tired of "real engineers", who are no more exact, informed or methodicai then programmers pretending that engineering is somehow less prone to exactly the same problems in project management and control as programming. It would a trival exercise to compile a list of engineering failures, just as it would be for programming failures. The real issue is how to design and manufacture anything correctly.

### Traffic Alert Collision Avoidance System with "no bugs"

Henry Schaffer <hes@uncecs.edu> Mon, 1 May 89 21:43:31 EDT

From: Assoc. Press article in the May 1, 1989 Raleigh(NC) Times:

The TCASSII system consists of a sophisticated transponder ... antennae, and a computer that analyzes and displays the movement of nearby planes. ...

"The system has no bugs," said Don Dodgen of Honeywell.

If two computers meet, he said, orders to the pilots will be reconciled automatically: if one plane is told to climb, the other will be advised to descend or to say on course.

No comment can do justice to this.

--henry schaffer n c state univ

## Nuclear reactor knocked offline by 2-way radio in control room

Wm. Randolph Franklin RPI <wrf@ecse.rpi.edu> Tue, 02 May 89 20:52:32 EDT

(condensed from Albany NY Times Union Wed April 26, 1989, page B-17)

The up-again down-again Nine Mile Point 2 nuclear power plant near Oswego was back on line Tuesday, following a weekend shutdown that "shouldn't have happened," according to a federal official.

An employee accidently keyed a hand-held two-way radio near circuitry for the turbine generator monitoring system Saturday night. The transmission shut down the system, which in turn triggered an automatic shutdown of the entire facility.

A section chief of the NRC region 1 office said that he has never heard of a similar accident but that most plants are sensitive and there are strict rules to prevent this.

Replacement fuel costs \$350K per day when the 1080 MW plant is down.

The plant had been up less than a week after a shutdown caused by corrosion and loose wiring in a meter.

#### B-2 builders: Prototype not needed (Long Article)

"Stephen W. Thompson" <thompson@a1.quaker.upenn.edu> Mon, 01 May 89 15:19:59 -0400

"Reprinted with permission from The Philadelphia Inquirer, April 24, 1989. Further reproduction of this article without the written permission of The Philadelphia Inquirer is strictly prohibited."

B-2 BUILDERS: PROTOTYPE NOT NEEDED

By Mark Thompson, Inquirer Washington Bureau

WASHINGTON - The builders of the Pentagon's B-2 Stealth bomber are boasting that their computer-aided design for the revolutionary boomerang-shaped aircraft is so good that the \$500 million plane will leap from the computer screen into the air by July without benefit of a prototype model to test the blueprints.

"The first B-2 is a production aircraft," the Northrop Corp. said in its just-released annual report. "There are none of the prototypes that have been required in previous generations of aircraft."

But critics warn that the Air Force decision to begin building the \$68 billion fleet of 132 sinister-looking planes before flight testing has even started could prove disastrous.

"I think the B-2 will crash the first time it flies," said Kosta
Tsipis, director of the Program in Science and Technology for
International Security at the Massachusetts Institute of Technology.
"I wouldn't be a passenger aboard it for anything in the world."

The lack of a prototype will make the planes' first flight "pretty exciting," agreed John Pike, associate director of the Federation of American Scientists in Washington.

"I'm perfectly prepared to see the airplane fly more or less as advertised," he said. "At the same time, I'm equally prepared to see the airplane crash more or less immediately."

But Capt. Jay DeFrank, an Air Force spokesman, said, "We're confident that it will make a successful first flight." The plane's two seats will be occupied by pilots from Northrop and the Air Force for the inaugural flight, which may occur secretly, he said.

The top-secret B-2, successor to the troubled B-1B, has been designed to fly into the Soviet Union undetected by radar. The not-ready-to-fly B-2, unveiled in November, is scheduled to be operational within the next several years, but Defense Secretary Dick Cheney said yesterday on NBC-TV's \_Meet the Press\_ that full production would not start in the 1990 fiscal year as planned.

Asked whether he would consider killing the program, Cheney replied, "We're going to postpone actually going into full procurement because I'm not comfortable with the program yet, there are a lot of technical problems with it, and it is extremely expensive. And until I have time to review it, which I've not yet had, I'm not prepared to make that judgement."

The B-2's flying-wing design is an updating of Northrop's YB-49 aircraft, a 1940s-era prototype bomber that the Air Force killed before production began. The B-2's shape is naturally unstable, and the lack of a tail means it will be much harder to control than a conventional airplane.

"It is essentially a boomerang," said James W. Kelley, a former Northrop aerodynamicist. "Once it goes into a spin, it cannot recover."

B-2 skeptics question both the plane's radical flying-wing design, first revealed a year ago, and the Air force's decision to save money by going straight from the drawing board to the production aircraft.

Historically, new aircraft designs are tested with a series of custom-built planes, each flown and modified until all major problems have been eliminated. Only then does production begin.

But in the case of the B-2, about a dozen planes are under construction, although not a single one has flown, several sources said.

In recent years, experts have urged the military to build prototypes to let them "fly-before-buy," confirming the designs before committing billions of dollars to production. Prototyping should be done "to uncover

operational as well as technical deficiencies before a decision is made to proceed with full-scale development," the presidentially appointed Packard commission said in its 1986 study critical of Pentagon purchasing.

But while the Air Force is requiring prototypes for its fledgling and highly secret Advanced Tactical Fighter, it does not believe the B-2 needs them.

"It was determined because of its revolutionary technology and the highly sensitive nature of the program that prototyping was not the best way to go," DeFrank said. The secret nature of the program prevented further elaboration, he said.

Others contend the plane's radical flying-wing design and high price tag demand prototyping.

"A \$70 billion program with no prototypes?" asked an incredulous Thomas S. Amlie, an Air Force engineer at the Pentagon, who said computers and models could not replicate the rigors of flight. "Of course we should prototype. We ought to fly one, and wring the hell out of it, with zero-zero ejection seats so the pilots can eject at zero altitude and zero air speed and live through it."

Amlie dismissed Air Force arguments that there were classified reasons why prototyping the B-2 makes no sense.

"They always say there are classified things that we can't know about because we don't have the clearance," Amlie said. "Well, I've been in the business for 37 years, and every time someone has told me that it turns out they were lying."

But Northrop says its battery of high-powered computers, whose data base contains drawings of all of the B-2's parts down to the smalles rivet, has "systematically eliminated" most of the risk inherent in a new aircraft design.

With the computers, design changes can be made before production begins. Such changes are particularly painstaking aboard the B-2, where the plane's radar-evading design requires a frozen exterior shape into which all of the plane's systems and weapons must be crammed.

"Given all the aerodynamic and performance compromises they've had to make to reduce the radar cross-section of the B-2, you're just flying much closer to the margin," said Pike of the Federation of American Scientists. "That's precisely why you need to do prototyping."

"It's very strange that they're not being required to prototype," added Joseph V. Foa, an aeronautical engineer at George Washington University who first studied flying wings 40 years ago. "When you have an aircraft that's going to cost a half-billion dollars apiece, it's a good idea to prototype.

Pike said recurring delays -- the plane's first flight originally was set

for 1987 -- showed that Northrop's computers had not eliminated the B-2's problems. "That tells me this thing is no different from anything else," he said. "Just because it looks right on the computer screen doesn't mean that it's going to work in the real world."

Without prototyping, the Air Force -- if it discovers problems -- will argue that the \$20 billion investment it already has made in the program requires repairs instead of cancellation, Pike said.

"They're basically front-loading the program so that regardless of what the test results are, they'll already have spent so much money on it that it will be difficult to cancel," Pike said. "You're paying to have the work done twice -- first time to do it wrong, and then the second time to do it right."

Stephen W. Thompson, (215) 898-4585 [no relation to Mark], Institute for Research on Higher Education, U. Pennsylvania, Philadelphia, PA 19104

## American Express is watching...

<sundar@mipos2.intel.com>
Thu, 4 May 89 15:59:53 PDT

Here is another addition to the list of risks of information age. There is an article in Thursday morning edition [May 4] of San Jose Mercury News titled "Member learns the hard way: American Express is watching". It described how American Express called a member to voice their concern that he might not be able to pay their recent bill. American Express was able to access his checking account and find that he had less than what was owed to them. His card was temporarily "deactivated" after the member refused to give any financial information except that he would pay up the bill with cash when it came in.

Apparently, the card application, in finer print, declares that "[American Express reserves] the right to access accounts to ascertain whether you are able to pay the balance". After some arguments with the company, the member comments that "I learned a lesson: My life is not as private as I thought".

First, this is news to me. I hold an AmExp card, and I wasn't even aware that my accounts are constantly being checked. Second, how could the banks dish out information on the account holders to third parties without proper authorization?

Sundar Iyengar, Microprocessor Design, Intel, Santa Clara, CA 95051

## Telephone line security

-David C. Kovar <corwin@daedalus.UUCP> Mon, 17 Apr 89 15:31:57 -0400

I was tracing the phone wires in my house yesterday afternoon trying to

find out why my phone was "off-hook" when all of the phones were actually hung up. Just before the lines enter my house I found a gray box labelled "Telephone Network Interface". Curious, I opened the box to find two RJ-11 modular phone jacks with black connectors in them that were held in by clips. I popped the clip, unplugged the plugs and plugged in a normal phone. Lo and behold, a dial tone! I wandered around the neighborhood a bit and found a few more of these boxes. Looks like you can wander around Boston with a phone, plug into someone's circuit, and make as many phone calls as you like. Who needs lineman's equipment?

-David C. Kovar, oOffice of Information Technology, Harvard University

#### COMPASS '89 Program

John Cherniavsky <jcc@mimsy.umd.edu> Thu, 4 May 89 15:21:06 EDT

```
* COMPASS '89 *

* JUNE 20th - June 22nd, 1989 *

* *

* NATIONAL INSTITUTE OF STANDARDS *

* AND TECHNOLOGY (formerly NBS) *

* Gaithersburg, MD *

* PROGRAM *
```

\* MONDAY, 19 JUNE 1989 \*

Meeting of the Tri-services Software Safety Working Group

```
* TUESDAY, 20 JUNE 1989 *
```

0730 REGISTRATION

0900 CALL TO ORDER, General Chair---Dario DeAngelis, Logicon

0910 OPENING REMARKS

Honorary Chair---The Honorable Tim Valentine,

Chairman for the House Subcommittee on Transportation

0930 PROGRAM OVERVIEW

Program Chair---John C. Cherniavsky, Georgetown University

0940 INTRODUCTION OF KEYNOTE SPEAKER AND PANEL

Chair, COMPASS Board---H.O. Lubbes, Space and Naval Warfare Systems Command

0950 KEYNOTE ADDRESS

"Computer Assurance: Safety, Security, Economics"

Allen Hankinson, National Institute of Standards and Technology

1130 KEYNOTE DISCUSSION

PANEL: Peter Neumann, SRI International Nancy Leveson, UC Irvine and MIT Allen Hankinson, NIST

Michael Brown, Naval Surface Warfare Center

1400 Special Presentation - Computer Related Risk of the Year

"Misplaced Trust in Computer Systems"

Peter Neumann, SRI International

1430 Minitutorial

"Formal Analysis of Safety"

Nancy Leveson, UC Irvine and MIT

1600 Software System Safety in the Military

Chair---Michael Brown, Naval Surface Warfare Center

\* Software Safety Handbook

Archibald McKinlay VI, McDonnell Aircraft Corporation

\* Role of the System Safety Manager in Software Safety,

Bruce Hill, Consultant

1730 ADJOURN

1900 BANQUET

\* "It is June 1989. Do you know what your computers are doing?" Peter Neumann, SRI International

\* WEDNESDAY, 21 JUNE 1989 \*

#### 0900 SOFTWARE SYSTEMS SAFETY:

Chair---Nancy Leveson, MIT and UC Irvine

\* Software Safety Goal Verification Using Fault Tree Techniques:

A Critically III Patient Monitor Example

Brian Connolly, Hewlett Packard

\* Using Petri Net Theory to Analyze Software Safety Case Studies

Wade Smith and Paul Jorgensen, Consultants

\* VMM Concepts Revisited

Marvin Schaeffer, Trusted Information Systems

1100 VERIFICATION, VALIDATION, AND TESTING

Chair --- Dolores Wallace, NIST

\* RM 2000 Approach to Software

Major Sue Hermanson, USAF

\* Condition Testing for Software Quality Assurance

K.C.Tai, North Carolina State University

\* Helping the Army Succeed Through Software V&V

Richard O'Reagan and Michael Edwards, Teledyne Brown Engineering

\* Experimental Evaluation of Six Test Techniques

Linda Lauterbach and B. Randall, Research Triangle Institute

#### 1430 NEW DIRECTIONS

Chair---Richard Hamlet, Portland State University

\* Access Control and Verification in Petri-Net Based

Hyperdocuments

P. David Stotts and Richard Furuta, University of Maryland

\* Unit Testing for Software Assurance

Richard Hamlet, Portland State University

\* Validation Through Exclusion: Techniques for Ensuring Software Safety

John C. Cherniavsky, Georgetown University

\* A Simple Way of Improving the Quality of Login Security

Khosrow Dehnad, AT&T Bell Laboratories

#### 1700 RISK ASSESSMENT

Chair---Janet Dunham, Research Triangle Institute

\*Risk Analysis: Case Studies of Two Approaches with an

**Expert System Based Tool** 

Jane Radatz, Logicon 1800 ADJOURN

\* THURSDAY, 22 JUNE 1989 \*

#### 0830 SYSTEM VALIDATION

Chair----Martha Branstad, Trusted Information Systems

- \* Techniques for Data and Rule Validation in Knowledge Based Systems Jong P. Yoon, University of Florida
- \* How to Qualify Knowledge Based Systems

Claude Vogel, Cisi Ingenierie

- \* Description of a Formal Verification and Validation Kenneth Lindsay, Magnavox Electronic Systems
- \* Taxonomy of the Cause of Proof Failure in Applications

Using the HDM Methodology

Kenneth Lindsay, Magnavox Electronic Systems

#### 1100 HARDWARE AND REALTIME VALIDATION

Chair----Thomas F. Buckley, University of Leeds

\* Programming a Viper

Thomas F. Buckley, University of Leeds

- \* Formal Verification of Microprocessor Systems
  - Mandayam Srivas, Odyssey Research Associates
  - \* Prospects for Verifying the PSN Code Stephen Crocker, Trusted Information Systems
  - \* Requirements for Process Control Protection John McDermott, Naval Research Laboratory

#### 1430 VERIFICATION OF SYSTEM FEATURES

Chair---H.O.Lubbes, Naval Research Laboratories

- \* Assurance for the Trusted Mach Operating System Martha Branstad, Trusted Information Systems
- \* Verifying Asymptotic Correctness

Mark Howard and Ian Sutherland, Odyssey Research Associates

- \* Security Analysis of a Token Ring Using Ulysses Daryl McCullough, Odyssey Research Associates
- \* Penolope: An Ada Software Assurance Editor Carla Marceau, Odyssey Research Associates

#### 1700 PANEL ---- ADVANCES IN FORMAL SOFTWARE ASSURANCE TECHNIQUES

Chair---John C. Cherniavsky, Georgetown University

Panel Thomas Buckley, Leeds University

Steven Crocker, Trusted Information Systems

Darryl McCullough, Odyssey Research Associates

Mandayam Srivas, Odyssey Research Associates

1800 ADJOURN

\* FRIDAY, 23 June 1989 TUTORIALS\*

#### 0900 TUTORIAL

\* A Guide to VIPER, A Verifiable Integrated Processor for Enhanced Reliability - or - Why, How, and Wherefore of Using a Formally Proved Microprocessor for High Integrity Control Systems

Thomas F. Buckley, University of Leeds

Jon Wise, Charter Technologies

0900 TUTORIAL

\* Formal Specification and Verification of Ada Programs David Guaspari, Odyssey Research Associates Carla Marceau, Odyssey Research Associates

1200 ADJOURN

FOR FULL REGISTRATION INFORMATION, SEND NETMAIL TO jcc@umd.mimsy.edu, or FTP KL.SRI.COM, get stripe:<risks>COMPASS.INFO. [I edited out the coffee and lunch breaks for brevity and nonredundancy. 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 8: Issue 67

**Sunday 7 May 1989** 

## **Contents**

Space software problems

**Henry Edward Hardy** 

Self-diagnostics in airplanes

**David Robinson** 

B-2 Builders: Prototype not needed

**Dave Parnas** 

**Bill Murray** 

**Henry Spencer** 

Standards == Nothing

**Dave Parnas** 

**Bob Estell** 

**Henry Spencer** 

Risks to contact lenses wearers from computer ventilators

Periklis Tsahageas

Re: Telephone line physical security

William M. Bumgarner

Mike Akre

Power lines and computers

George Michaelson

Not using computer helps trapping of error

**Konrad Neuwirth** 

Info on RISKS (comp.risks)

#### Space software problems

<Henry\_Edward\_Hardy@ub.cc.umich.edu> Fri, 5 May 89 11:35:48 EDT

New York Times Reports Shuttle Software Patch

Excerpted from the New York Times 5-5-89 edition by Henry E. Hardy

[...] In checking the Magellan's control systems two weeks ago, engineers detected and corrected one potentially catastrophic problem. A design flaw was found in the software for the spacecraft's computer. If the craft were to lose its proper orientation to the Sun and the Earth, the flaw could have prevented the spacecraft from regaining its bearings. The result could have been the loss of the spacecraft, as it failed to get enough solar energy to run its electronics and thus could no longer keep its antenna pointed at to Earth.

Project officials said engineers devised a "patch," a substitute set of instructions, to override the design flaw.

John H. Gerpheide, the Magellan project manager at the Jet Propulsion Laboratory in Pasadena, Calif., said: We're convinced that we've got a good fix on the problem. The fix has been tested and thoroughly reviewed. We don't have any concern at all."

Errors in computer instructions were said to have been the cause of the failure of Phobos 1, an unmanned Soviet spacecraft, as it was headed to Mars last September. The spacecraft tumbled out of control. And the craft, unable to keep its solar panels pointed to the Sun, ran out of electricity.

The companion craft, Phobos 2, made it to an orbit of Mars and then failed as it was maneuvering to drop scientific instruments on the tiny Martian moon Phobos. Soviet scientists who were here to view the launching of the Atlantis said the cause of the Phobos 2 loss was still unclear.

### Self-diagnostics in airplanes

David Robinson <david@elroy.jpl.nasa.gov> 7 May 89 02:11:24 GMT

Here is a NASA press release on a self-diagnostic \*IN FLIGHT\* maintenance system. I am sure this would be useful in tracking down problems but I can only imagine the problems that could arise from trusting such a system.

"But the computer said it was fixed"

-David Robinson

NASA FLIES FIRST AIRCRAFT SELF-DIAGNOSTICS SYSTEM ( RELEASE: 89-69 )

In the first flight in a joint NASA/USAF program that promises self-repairing flight controls and lower maintenance costs in future aircraft, computers aboard the NASA Ames-Dryden F-15 Flight Research Aircraft were able to correctly identify and isolate in flight a simulated failure in the flight control system.

Flight control system failures can and do occur during flight. When this happens, costly ground maintenance diagostic tests are conducted to try to identify the failure so that appropriate corrective actions may be taken. In many cases, the failure cannot be identified during ground tests because the actual flight conditions are not duplicated. With the new expert system technology, failures can be identified and isolated before landing and be fixed immediately.

The first simulated failure was an angle-of-attack sensor. The

maintenance diagnostic system correctly identified the failure and isolated the problem. Future tests will incorporate other failures.

"This is a real breakthrough in flight control system maintenance diagnosis for future aircraft," says F-15 Flight Research Aircraft Project Manager Dr. James Stewart. "Newer digitally-controlled aircraft are more complex. However, digital controls allow this type of computer programming which will reduce the maintenance cost of future digitally-controlled aircraft."

The maintenance diagnostic system is the first technology to be tested in the Self-Repairing Flight Control Program. The other technologies, scheduled to begin flight tests this fall, include failure detection, identification and reconfiguration of the flight control system.

An example of the need for reconfiguration is when a tail surface fails in flight. The flight control system will be reconfigured (repair itself) so that other surfaces take over the function of the failed tail surface. Also, a pilot alert system will tell the pilot what the problem is and what the new configuration and flight envelope are after the system has self repaired.

This program is being conducted by NASA's Ames-Dryden Flight Research Facility, Edwards, Calif., and is sponsored by the Air Force Wright Research and Development Center, Wright-Patterson Air Force Base, Ohio. The prime contractor, McDonnell Aircraft Company, St. Louis, Mo., with the General Electric Aircraft Control System Division, Binghampton, N.Y., designed and developed the maintenance diagnostic system for use in the NASA program.

#### B-2 Builders: Prototype not needed

Dave Parnas <parnas@qucis.queensu.ca> Fri, 5 May 89 08:17:55 EDT

I found the fuss about Northrop's statement that the first B-2 will be a production aircraft to be unjustified. The mere fact that they say it is not a prototype does not mean that it is not a prototype, My dictionary defines "prototype" as a first or early example of something. Nobody is claiming that the first will be the second or a late example of the B-2. Whatever they call it, the risks will be the same. Some organisations and spokesmen will use any excuse to stir up a controversy.

David L. Parnas

## Prototypes

<WHMurray@DOCKMASTER.NCSC.MIL>
Fri, 5 May 89 08:24 EDT

Software engineers please do not be misled. It is not the generation nor even the design that requires a prototype. The prototype is part of the design. The design is not complete without it. All assertions to the contrary are

fallacious and dangerous.

Engineering of any kind is risky enough without this kind of foolishness.

William Hugh Murray, Fellow, Information System Security, Ernst & Whinney

## ★ Re: B-2 builders: Prototype need not apply

<henry@utzoo.UUCP>
Sun, 7 May 89 07:58:49 -0400

There is a subtlety here that people not intimate with military aviation may not appreciate. This is not as big an innovation as Northrop is claiming. It has been common for quite some time to build even the first one of a new aircraft in "production" tooling. Although it does save a lot of time, it also contributes greatly to realistic testing. Things like production processes affect the result; it simply is not possible, in practice, for a hand-built prototype to accurately represent production hardware. Proper testing requires hardware built with production tooling. This practice started with the USAF's "Cook-Craigie plan" techniques in the 1950s.

(Many of the critics quoted in the Philadelphia Inquirer article are making fools of themselves because they don't understand this.)

Doing this also helps a lot when one wants to get production moving rapidly after testing; part of Cook-Craigie is a scheme whereby early stages of production ramp up fully while later stages concentrate on getting the first few aircraft out the door, the hope being that any modifications that are needed will not affect the early stages badly.

Inevitably, this sort of thing involves risk that production tooling will need to be torn up and revised because testing finds problems, and that half-built aircraft may need expensive revisions or even scrapping. Efforts are made to get the thing right the first time, and to get good test results as quickly as possible. Sometimes it works well; sometimes not. As in other such production innovations, after early successes there was a tendency for later projects to get the outline right -- first aircraft built in production tooling, first stages of production rolling early -- while forgetting important unorthodox details like the emphasis on intensive early testing. The result is failures, which tend to be blamed on bad luck or the inherent difficulty of the problem rather than on bad management.

(Another production innovation which suffered the same fate was concurrency: designing all the pieces of the hardware simultaneously, relying on good interface documentation to make sure they all work together. When it works, it gets hardware out the door much sooner than step-by-step methods. It worked well for the early ICBM programs because (a) they consistently funded multiple parallel development efforts for anything deemed risky, and (b) they didn't choose between them until hardware was available to be tested. Many later programs adopted concurrent development without these important (and expensive) details, the result being a lot of failures.)

The ultimate end product of remembering the successes but forgetting the details is what's going on at Northrop: the conviction that it's possible to get everything right the first time, so no modifications will be needed and full-scale production can start immediately. That \*is\* folly, but not because there aren't any prototypes.

Henry Spencer at U of Toronto Zoology

#### Standards == Nothing

Dave Parnas <parnas@qucis.queensu.ca> Fri, 5 May 89 08:07:27 EDT

Rich Neitzel's anecdotes do not justify his conclusion. In every case that he mentioned there were standards that were clear enough and substantive enough that, in his opinion, they were not met by the products in question. We have no such standards in software. He points out that we will never eliminate fraud and incompetence. The fact that there will always be people who cheat does not mean that we should not have standards. Au contraire!

Dave Parnas

#### Bad standards are still better than nothing

"FIDLER::ESTELL" <estell%fidler.decnet@nwc.navy.mil> 5 May 89 09:12:00 PDT

"A bad standard is better than nothing. It gives you something to violate." [A quote from the Hammer Forum, 1986]

"Standards are like motherhood: They should not come too soon, and there should be an identifiable father." [CAPT John Nichols, USN, 1968]

Gordon Bell said it best in his seminal essay, "Standards Can Help Us," IEEE COMPUTER, June 1984, pp. 71-78. Serious readers should review that article.

The practical application of the tongue-in-cheek advice from Hammer '86, and from Nichols and Bell, is that at the least, standards, even flawed ones, give us the basis for further discussion, based on something more than just personal taste. I remember discussing computer system reliability with representatives of UNIVAC, early in this decade. These capable folks had arguably one of the best systems of that era - the UNIVAC 1100 series. Its ancestors had succeeded despite a history of frequent crashes, which were then common in the industry. Newer systems, with designs unhampered by demands for "backwards compatability" with older models, and free to use newer technology, were beginning to demonstrate an order of magnitude more reliable performance; e.g., one crash a quarter instead of one per week. (Actually, the old systems were worse than that, and the new ones better.) I lost that argument, because the others were convinced that "bigger means less reliable." An analogy about jumbo jets vs. smaller plans did not help. It was only when the competition [viz., IBM] introduced the 308x series, with its multi-megabyte diagnostic code, and MTBF in months vice hours, that the argument was over.

I'm not suggesting a "standard for reliability." I am saying that the effort to make standards can help us appreciate the diversity of our needs, and the adoption of standards can raise our level of expectations.

## ★ Re: Use of "Standard" on sensitive applications

<henry@utzoo.UUCP>
Wed, 3 May 89 23:15:27 -0400

Generally rather similar to the risks involved in using other "standard" tools like compilers, assemblers, text editors, front-panel switches :-), operating systems, etc.: there is always a chance that the tool has not been fully tested and will do the wrong thing silently, or that it will not catch user errors that it is supposed to catch.

>Is it reasonable to set some criteria ...

Lengthy use tells you something about the average density of bugs in the code, but won't necessarily tell you about the one bug that's in precisely the wrong place. Thorough validation suites are better, although rarer.

Better yet are validation suites for the \*application\*, ones which do their best to stress its components. (Note, this is not the same as "black box" validation suites written with no knowledge of said components.) The fact is, even well-proven tools can have obscure bugs lurking in them. Case in point: the C compiler in V7 Unix, an unambitious compiler written by a very good programmer and exhaustively shaken down by widespread use, had a bug in its 32-bit-divide routine that was not found until people -- specifically, some of my users -- stumbled over it. The code made some assumptions about the hardware that were true, at least most of the time, of older pdp11 processors but not of the new 11/44 we had. The most interesting part was that my fix for the problem appears to have also cured some much rarer misbehavior found even on older processors. The values returned by that routine may have been wrong, occasionally, all along.

One simply cannot afford to place implicit trust in \*any\* of the tools used to build a sensitive application. As with "end to end" arguments in networking, to be sure that the final product is right, one must test it directly and not rely on trusted tools.

Henry Spencer at U of Toronto Zoology

#### Risks to contact lenses wearers from computer ventilators.

Periklis Tsahageas <periklis@ecrcvax.UUCP> Fri, 5 May 89 11:30:13 +0200

About a month ago, I moved to my office, in my new job. A sun 3/140 workstation was on my desk. Being more of a thoeretical person, I barely touched it. The first day at work hadn't finished and I had a strong discomfort in my left eye. When I went home, I had to take my contact lenses

out immediately. Next day at work, the discomfort became even stronger. I have been wearing contact lenses for seven years now but had never felt something like that before. This continued during the whole week.

On Saturday, I was surprised to discover that the discomfort had almost gone. On Sunday, I was feeling perfect. This prompted me to think that it had something to do with my work. The arrangement on my desk is as follows (view from the top):

As you can see, (you should be able to :-)) my head is in the path of the stream of air coming from the ventilation holes (:) of the sun. This air, not only has a large enough speed (if you put your hand in front of my face, you can sense the draft) but also is dryer, hence has lower relative humidity, than the rest of the air in the room. This means that it dries my contact lenses a lot faster than usual. I think this was the cause of the discomfort.

In order to try my hypothesis, on Monday morning, I blocked the ventilation holes, using a triangular calendar that was on my desk, as follows (front view, as if you are sitting in front of the computer):

As you can see, the draft is now redirected sideways, away from me, and I don't have any problems anymore. The Sun should be O.K. since the one inch minimum ventilation clearance, required by the manufacturers, is satisfied. Of course, you could argue that if I was hacking away on my sun, the draft would not fall on me, which makes this a RISK of NOT using a computer :-).

Periklis Andreas Tsahageas European Computer-Industry Research Centre Arabellastrasse 17, D-8000 Muenchen 81, West Germany +49 (89) 92 69 91 09 Europe: periklis@ecrcvax.uucp ...!unido!ecrcvax!periklis

Re: Telephone line physical security [Kovar, RISKS-8.66]

"William M. Bumgarner" <wb1j+@andrew.cmu.edu> Fri, 5 May 89 07:54:40 -0400 (EDT)

Not only is it possible to pop off the grey cover and use the diagnostic modulars that are commonly found on the sides of houses (or the nearest telephone pole), but it is also possible to access nearly every line in an area of a city fairly easily. Simply find one of the grey boxes usually at the base of a phone line tpole where the cable switches from above ground to below ground. These junction boxes will usually have x0,000 thousand twisted pair lines connected together and hanging over a metal bar. Simply pick one, and patch in w/a pair of aligator clips. This can also be done inside of the black covers hanging on telephone poles.

If you really want to create some havoc, cut a couple of twisted pairs in really hard to reach places...

On a related note, a story:

Our neighbor's hired some people to come in and clean their house. It was done in a rather odd fashion; you call a friend of the cleaners who then told the person that someone called for them. The cleaner would then return the callbut would never have a number that they could be reached at. No big deal, they were using a pay phone.... wrong. The person had a phone w/ aligator clip instead of RJ-11 male connnector in a bucket. Acting like they were pruning the bushes, they would tap a neighbor's line and call whenever they needed....

It really does happen!

#### Re: Telephone line physical security

<cuuxb!akre@att.att.com>
Fri, 5 May 89 14:03:34 EDT

Whenever my local telephone company (Illinois Bell) installs new service or alters existing service they move the telephone network interface outside. They do this to simplify their access for testing.

When I had a second telephone line installed at my home, the installer was about to replace the existing network interface in the basement with a gray box outside. It took me some time to convince the installer to put the network interface inside.

Mike Akre, AT&T, Lisle, IL

#### power lines and computers

George Michaelson <ggm@brolga.cc.uq.oz.au> Fri, 05 May 89 13:04:01 +1000

I have just discovered that our local Electricity Supply Company is using PC's and now even X-windowed VMS & Unix systems to bring circuits

up and down: an iconic display allows a mouse-click and a keyboard confirm to activate a circuit breaker, through comms links to the grid.

Apparently NO physical token exchange is used between linespeople and controllers: A verbal confirmation, coupled to somebody watching the breaker come in or out is all that is used.

Perhaps I'm being too paranoid, but If I were a linesman I'd want to see the key for that segment in my hands before I climbed the tower, much as permanent way crews do (used to?) for track repairs, or train drivers for bi-directional single-line working.

Should automated systems maintain physical key/token exchanges from the past? is there an electronic "equivalent" that could be used instead?

On the plus side, They're using Radar scans of lightning strikes and the PC network to offer some predictive services: they try and direct line-crews to be on the alert \*before\* a storm reaches their section.

On the whole I think the use of computers, especially bitmapped displays is beneficial in this area: they can condense a lot of information into one screen, in a simple and intuitive form. Of course, providing some active control has an "inverted" effect: simple mistakes can propagate out into catastrophies.

George Michaelson, Prentice Computer Centre, Queensland University, St Lucia, QLD 4067

#### Not using computer helps trapping of error.

Konrad Neuwirth <A4422DAE%AWIUNI11.BITNET@CUNYVM.CUNY.EDU> Sun, 30 Apr 89 12:29:20 MEZ

Last week, I went to our local bank to do a money transfer to an american bank. Though the clerk had a terminal on her desk, she fetched a typewriter and had to type everything on a paper form. This surprised me a bit as the bank says they are very up to date with technology, but that's something else. I gave her a piece of paper with all the addresses on the one side (recipient and bank), and on the other side, there was the bank routing number and the account number. I thought she had done everything all right, took my copy of the form, paid the thing and went home. When I came home, the bank had already closed as it was 18.25. I took the form out and discovered that she had not filled in the bank routing number. This made me curious and I took out my little paper and checked the form... BINGO! I found out that she had written the address of the recipient correctly, but had written the zip code of the bank as the account number and no bank routing number, except: Household Bank, Columbus, Ohio. Next morning I ran to the bank and told them about this. They immediately called their headquaters as all those forms are sent of after the bank closes. Luckily, they could take the form out of the stack and everything was all right. The clerk said: "Oh, there was something on the back side, too? I only read the front side.". She didn't even notice!

But imagine if the computer had done this immediately... either the computer would have rejected the input or I could have paid the whole thing twice..

Konrad Neuwirth, Fernkorngasse 44/2/4, A-1100 Wien, Austria



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 8: Issue 68

Monday 8 May 1989

#### Contents

- Low-Probability / High-Consequence Accidents -- and the Midland 737?
- "Probing Boeing's crossed Connections" Werner Uhrig
- An Atlantis spacecraft computer problem resolved nicely
- "Life's Risks: Balancing Fear Against Reality of Statistics" Marc Rotenberg Jerry Leichter
- Hear No Evil

**Kevin Driscoll** 

- Computer Ethics Course/Resource Volunteers Wanted (long) **Bob Barger**
- Info on RISKS (comp.risks)

### ✓ Low-Probability / High-Consequence Accidents -- and the Midland 737?

Peter Neumann < neumann@csl.sri.com> Mon, 8 May 1989 8:34:12 PDT

I would like to consider here a class of problems that has not been addressed specifically in RISKS, although its components are familiar. The RISKS Forum has addressed alarm systems that could not adequately be debugged under truly real circumstances. There was also the example of the earliest Antarctic ozone depletion data, which was systematically rejected by the analysis program for being \*too\* anomalous. The potential for a combination of these two types of problems might occur in aircraft monitoring during flight, as follows.

Sensitive sensors in hostile environments (such as engines) sometimes report unrealistic or off-scale readings due to noise or interference. Consequently software monitoring the sensor may be programmed to ignore values beyond a certain threshold, on the grounds that such extreme readings must be the results of extraneous events. If the ignored sensor reading was "real", however, other more remote sensors might pick up -- and accept -- less extreme readings. This appears to be a potential problem in a variety of control systems.

In the absence of any definitive information about the British Midland 737 crash, such a hypothesis seems just as plausible as any other. The \*left\* engine was reportedly vibrating wildly (possibly due to a broken fan blade), but the pilots for some reason(s) shut off the (good) right engine. The extreme vibration in the left engine might indeed have produced hitherto unexperienced sensor readings that designers -- or the software folks -- felt would have to be impossible. The vibration from the left engine would have been transmitted -- much attenuated -- through the entire airframe, and might have been reported at a much more "reasonable" intensity by the vibration sensors of the right-hand engine. It does not take much of a leap in imagination for the computer program to conclude that it was the \*right\* engine that was malfunctioning.

In any event, this possible fault mode represents another case of LOW-PROBABILITY / HIGH-CONSEQUENCE ACCIDENTS [1], and thus deserves explicit attention. Unfortunately it is just one more such combinatory fault mode.

[1] See Koshland's editorial (title above, in CAPS) in Science, vol 244 no 4903, 28 April 1989, p. 405, discussing the Exxon Valdez spill and conclusions that should be drawn from it.

## "Probing Boeing's crossed connections"

Werner Uhrig <werner@rascal.ics.UTEXAS.EDU> Mon, 8 May 1989 4:53:45 CDT

[The title is that of an article in IEEE Spectrum, May 1989, pp. 30-35, subtitled ``Misconnected circuits and hoses found on 94 in-service Boeing aircraft raise concern about design, test, and maintenance of aircraft safety systems". Author is Karen Fitzgerald.]

At the very end of the article is a further reference of interest to this group:

For a minute-by-minute account of the British Midland crash from knowledge gathered to date, see Special Bulletin S2/89 of the Air Accidents Investigation Branch of the Department of Transport in Farnborough, England, March 20, 1989.

[I recommend the Spectrum article, and would like to see the Bulletin. PGN]

## An Atlantis spacecraft computer problem resolved nicely

Peter Neumann <neumann@csl.sri.com> Mon, 8 May 1989 12:13:25 PDT

One of Atlantis' main computers (one of the processors in the two pairs of the

2x2 + 1 backup architecture) failed on 7 May. For the first time ever the astronauts made repairs -- in this case by substituting a spare processor. It took them about 3.5 hours to gain access to the computer systems by removing a row of lockers on the shuttle mid-deck, and another 1.5 hours to check out the replacement computer.

It is ironic that such a replacement was so difficult, but not surprising. My old friend Al Hopkins, who at MIT Instrumentation Lab (now Draper Lab) designed the Apollo on-board guidance computer, told me years ago how carefully they had planned the packaging so that the astronauts would be able to make repairs on the fly (as it were). NASA officials would have none of it, and buried the computer several layers underneath other equipment. Apparently that tradition has continued. Perhaps the success of the Atlantis crew will change things.

During STS-9, Nov-Dec 83, multiple primary computers on the Columbia failed at the same time, and delayed the return to earth. On one hand, the calculations say that losing three processors would be a rare event. However, here we have another example of a low-probability / high-consequence accident -- especially if it involved the backup and one of each of the pairs. Furthermore, since the software is the same in all four of 2x2 the main processors, they would all have failed consistently, and been deemed correct. (And we just reported the serious problem in the Magellan software caught before Atlantis' launch, noted in RISKS-8.67!) In the case of pairwise disagreement among both pairs, there is always the fifth, backup, computer, separately programmed. As far as I know, the shuttles have never had to rely on the backup computer software, so it might be preferable to make processor replacements among the main four rather than resort to the backup...

### "Life's Risks: Balancing Fear Against Reality of Statistics"

Mon, 8 May 89 12:14:37 -0700

Excerpted from today's New York Times:

Is the slight risk of contracting cancer from Alar too high a price to pay for crisper apples? Is the dramatic increase in milk production available through genetically engineered growth hormones worth the unknown risk to children's health? If a few aging aircraft suffer explosive decompressions, should all old airlines be grounded?

Risks to health and safety and the complex questions of public policy they create are seemingly everywhere these days. And while there is little statistical evidence that the hazards of daily life are on the rise, a wide range of academic and business experts believe that American's perception of increased peril is stifling technology, wasting billions of dollars, and, ironically, making it more difficult to contain the most serious risks.

... by broad statistical measures, Americans have never been safer ...

Even the high-profile threats have not changed the risks of untimely death or injury. The skies may be crowded, the planes aging and the pilots inexperienced, but the trend in aircraft fatalities is downward. ...

Life-saving medicines have been less dramatically affected, but even here, the measures to compensate for risk can radically change the economic of distribution ...

The Environmental Protection Agency also regards itself as handicapped by Congressional and public misperception of relative risk. ...

What explains the public's decreasing tolerance of some risks and apparent indifference to others? ... perceived risk is not always related to the probability of injury.

Easily tolerated risks include ones that people can choose to avoid (chain saws, skiing), that are familiar to those exposed (smoking), or that have been around for a long term (fireworks). Poorly tolerated risks are involuntary (exposure to nuclear waste), have long delayed effects (pesticides), or unknown effects (genetic engineering).

... nuclear and chemical technologies fare especially badly in such subjective rankings. Indeed the general acceleration of technical change and integration of new technology in products helps to explain the increase in public anxiety about risk. ...

#### Life's Risks ...

LEICHTER-JERRY@CS.YALE.EDU <"Jerry Leichter> Mon, 8 May 89 17:17 EDT

Today's New York Times (Monday 8 May) has a front-page article title "Life's Risks: Balancing Fear Against Reality of Statistics". It's the first of two articles on "risk and public policy".

The article is ... well worth reading. Here's an interesting quotation:

Peter W. Huber, and engineer, lawyer and author of "The Legal Revolution and its Consequences" notes that ... "safety taxes" [extra costs charged by suppliers to pay for potential lawsuits] are added to the price of thousands of ... goods and services, distorting production and reducing living standards. By Mr. Huber's reckoning, the safety tax represents 30 percent of the cost of a step ladder, one-third the cost of a ride on a Long Island tour bus and \$300 of the cost of giving birth in New York City.

-- Jerry

## ✓ Hear No Evil

Kevin Driscoll <driscoll@draco.src.honeywell.com> 7 May 89 22:44:01 GMT

On a recent flight, the cabin crew was a bit late in starting the in-flight movie. The flight took less time than expected, so the movie's climactic showdown scene began just after plane touched down. Many of the passengers

became noticeably irritated at the flight attendants pre- and post-landing announcements which interrupted the movie's audio. This was a tow-in gate so the engines were shut down well before arriving at the gate. Without engine power, an APU supplies electrical power. On the switch-over, however, the power glitch reset the audio channel controllers to the default channel (8) which is silent. It is common on commercial aircraft to have "unimportant" control systems (such as the individual seat lighting and audio) reset on power glitches. This is not a safety problem. Is it?

When the audio went dead on this flight, most of the passengers didn't know what happened and pushed their flight attendant call buttons. Same of the more irate passengers repeatedly pushed it, causing the alert tone to sound almost continuously. (This was what I could see in first class. I can only imagine what was happening in the coach cabin where passengers had to explicitly pay extra for headsets and where there were more passengers.)

I would suspect that the official justification for the flight attendant call button system is to alert the crew to emergencies. During this incident, any signaling of an emergency would not have been noticed. I also suspect that a failure analysis of the audio system did not foresee the implications of a power glitch reseting the channel. This is an example of the most common reason for safety problems; the designers don't see all the possible circumstances that the design will face, particularly where people are involved.

The fix to this problem is trivial; make the default channel one with some material on it, preferably one of the movie channels (1 through 4). I wonder if the current design was to save some small amount of power.

Another disconcerting observation was that the cabin crew did not seem to understand what had happened either. They seemed unable to help the passengers. They made repeated visits to the passengers who contined to re-press their call buttons. All that had to be done was to switch the channel back to where it had been.

Disclaimer: I don't represent Honeywell, neither should Don Dodgen.

Kevin R. Driscoll, Principal Research Scientist (612) 782-7263 FAX: -7438 POST: Honeywell M/S MN65-2500; 3660 Technology Drive; Mpls, MN 55418-1006

#### Computer Ethics Course/Resource Volunteers Wanted

Bob Barger <CFRNB@ECNCDC.BITNET> Wed 03 May 1989 13:51 CDT

Two drafts of the following course were previously printed in RISKS digests. These brought a host of suggestions from readers. Almost all these suggestions were incorporated into the final version below. Volunteers are now being sought to participate in the course this Fall (see Section 3. b. 2. below). These volunteers could contribute items relating to computer ethics for posting on the class bulletin board, correspond by e-mail with individual students on course topics, and/or comment on students' postings on the class bulletin board.

The course will run from late August to early December. No money is presently available as compensation for this service, but I will gladly contribute letters of appropriate recognition for those who participate as resource persons in all or part of the course. If interested, send a brief "vita" to Bob Barger at CFRNB@ECNCDC.BITNET.

# SENIOR SEMINAR EASTERN ILLINOIS UNIVERSITY

#### 1. Catalog Description

a. Course Number: EIU 4050

b. Title: Computer Ethics

c. Credit: 2-0-2 [2 hrs per week/one semester]

d. Term to be offered: On Demand

e. Short title: Computer Ethics

- f. Course Description: The course will investigate current ethical issues involving computers. While it is not a "computer course," students will make frequent use of postings on the electronic bulletin board of the ECN mainframe computer to research and discuss ethical issues.
- g. Prerequisites: 75 Semester Hours and previous experience with computers. [Class size limit = 15 students for Fall, 1989, semester].

h. Exclusions: None.

#### 2. Outline of topics:

#### Week Topic

- Orientation to the course (introduction, explanation of course content, class procedures, and evaluation methodology). Consideration of ethical theory: examination of the metaphysical bases and resultant ethical norms of the idealist and naturalist theories.
- 2 Consideration of ethical theory (continued): examination of the metaphysical bases and resultant ethical norms of the consequentialist and existentialist theories.
- On-line reading of the "Discussion of Ethics in Computing" list, the "Forum on Risks to the Public in Computers and Related Systems" digest, and the "Computers and Society" list (all are available on

the ECN bulletin board); written reactions to these readings, and written commentary on other students' reactions. [The instructor will insure that these activities equate to the activities of a traditional two hour class meeting].

- Consideration of professional ethics: responsibilities between employer/employee, client/professional, professional/peer, and professional/society.
- On-line reading of the "Discussion of Ethics in Computing" list, the "Forum on Risks to the Public in Computers and Related Systems" digest, and the "Computers and Society" list (all are available on the ECN bulletin board); written reactions to these readings, and written commentary on other students' reactions. [The instructor will insure that these activities equate to the activities of a traditional two hour class meeting].
- 6 Consideration of liability for software design, manufacture, and use: legal liability; truth-inadvertising; contracts; warranties; software as product or service?
- On-line reading of the "Discussion of Ethics in Computing" list, the "Forum on Risks to the Public in Computers and Related Systems" digest, and the "Computers and Society" list (all are available on the ECN bulletin board); written reactions to these readings, and written commentary on other students' reactions. [The instructor will insure that these activities equate to the activities of a traditional two hour class meeting].
- 8 Consideration of privacy issues: individual privacy rights; institutional "right-to-know" concerns; system security concerns; data-banking concerns.
- On-line reading of the "Discussion of Ethics in Computing" list, the "Forum on Risks to the Public in Computers and Related Systems" digest, and the "Computers and Society" list (all are available on the ECN bulletin board); written reactions to these readings, and written commentary on other students' reactions. [The instructor will insure that these activities equate to the activities of a traditional two hour class meeting].
- 10 Consideration of power/control issues: the computer as agent of centralization or

decentralization? the computer as agent of conservation or change? the computer as agent of alienation?

- On-line reading of the "Discussion of Ethics in Computing" list, the "Forum on Risks to the Public in Computers and Related Systems" digest, and the "Computers and Society" list (all are available on the ECN bulletin board); written reactions to these readings, and written commentary on other students' reactions. [The instructor will insure that these activities equate to the activities of a traditional two hour class meeting].
- 12 Consideration of ownership and theft issues: copyrights; fair usage; patents; trade secrecy and competition; considerations unique to the computer market.
- On-line reading of the "Discussion of Ethics in Computing" list, the "Forum on Risks to the Public in Computers and Related Systems" digest, and the "Computers and Society" list (all are available on the ECN bulletin board); written reactions to these readings, and written commentary on other students' reactions. [The instructor will insure that these activities equate to the activities of a traditional two hour class meeting].
- On-line reading of the "Discussion of Ethics in Computing" list, the "Forum on Risks to the Public in Computers and Related Systems" digest, and the "Computers and Society" list (all are available on the ECN bulletin board); written reactions to these readings, and written commentary on other students' reactions. [The instructor will insure that these activities equate to the activities of a traditional two hour class meeting].
- 15 Seminar members will reconvene as a group for the last meeting to allow for group reflection on the seminar experience and course evaluation.

Exam week Final examination

Writing component

Students will type thirteen 30-to-50 line (i.e., one-to-two page) reactions to the on-line electronic bulletin board readings. Students will "post" these reactions (i.e., electronically send them to the mainframe computer bulletin board set aside for members of this seminar). In their reactions, students will: 1) identify the particular publication or publications to which they are reacting, 2)

identify the particular issue or issues raised in the publication(s), 3) identify the ethical implications of the issue or issues, 4) identify the ethical paradigm used by the author, 5) add their own reasons for agreement or disagreement with the viewpoint of the publication's author, 6) and, finally, offer an alternative solution or viewpoint to that presented by the author, or present other appropriate considerations not raised by the author or covered in their own (i.e., the student's own) previous comments. The instructor will send weekly, by confidential electronic mail, a grade on the student's posted reaction, together with whatever comments the instructor thinks helpful. The student's original posted reaction will also be open to public comment by the other students in the seminar [this is accomplished by posting notes to the bulletin board, referencing the original posted reaction]. These latter comments by the other students in the seminar will be considered along with classroom discussion in computing the "participation" factor of the student's semester grade.

#### Evaluation

Each student's semester grade for the seminar will be calculated according to the following weighted formula:

- 13 posted reactions (at 5% each) = 65%
- Participation (based on class discussion and posted comments on other students' reactions) = 20%
- Final Exam = 15%
- 3. Implementation :
  - a. This course will be taught by: Robert N. Barger, Ph.D.
  - b. Materials in the course will include:
    - 1) Texts:
      - a) Deborah Johnson, Computer Ethics (Englewood Cliffs, NJ: Prentice Hall, 1985)
      - b) Notes on Systematic Philosophies from Dr. Barger's Philosophy 1800 class (furnished without charge to seminar members)
      - c) Postings on the above-mentioned ECN electronic bulletin board lists.
    - 2) Resource people: Computer professionals (e.g., administrators, systems analysts, programmers, etc.) will be utilized as guest contributors to the class. This will be accomplished by personal appearances, as well as by electronically mediated conferencing (e.g., postings, e-

mail, relay round-tables, etc.).

c. Exceptional costs: None, unless the student wishes to use a modem to access the computer. In this case the student will be responsible for any personal equipment costs and/or long distance phone charges.

d. Effective date: Fall, 1989.

Date approved by Senior Seminar Committee: February 24, 1989.

Date approved by Council on Academic Affairs: April 20, 1989.



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 8: Issue 69

## Wednesday 10 May 1989

## Contents

Computers and Redistricting

**PGN** 

Re: Atlantis spacecraft computer problem resolved nicely **Henry Spencer** 

Computer-generated checks

**Art Werschulz** 

Re: Hear No Evil

Clay Jackson

Computer Bugs/Recalls/Upgrades Clay Jackson

Info on RISKS (comp.risks)

## Computers and Redistricting

Peter Neumann < neumann@csl.sri.com> Mon, 8 May 1989 17:18:03 PDT

I have had several high-level inquiries lately concerning census database privacy/confidentiality/integrity, and integrity of the analysis used to govern redistricting -- as well as more on the confidentiality and integrity of computer systems used in elections. There are several risks worth noting here.

- \* Early knowledge by one party of census data could be used to plan appropriate gerrymandering and campaign strategies.
- \* Manipulation of census data (in gathering, computer data entry, and storage) could influence redistricting, at both state and federal levels.

One of my recent visitors was ostensibly interested in protecting the redistricting process from tampering (through legislation, oversight, etc.), but I had a nagging feeling that there might also conceivably have been some interest in how that process could be subverted. 1992 is not too far away, so it seems appropriate to raise these problems now.

### ★ Re: Atlantis spacecraft computer problem resolved nicely (RISKS-8.68)

<henry@utzoo.UUCP>
Tue, 9 May 89 12:51:39 EDT

- > NASA officials ... buried the computer several layers underneath other
- > equipment. Apparently that tradition has continued...

NASA has a considerable tradition of implicitly assuming that the only failures that can happen are the ones in the book. For example, it was pure luck that the Apollo 13 astronauts survived, because that particular type of accident --Service Module systems completely dead -- had been classed as unsurvivable and no preparations had been made for it. Using the Lunar Module's life-support systems for most of a mission required using Command Module lithium-hydroxide canisters in the LM... and the two were not mechanically compatible, and no adapter was provided (one was improvised). Using the LM computer to navigate home was possible only because one or two people at MIT had loudly insisted that the CM and LM computers should be identical. Nobody had ever thought about how to separate CM from LM without the SM maneuvering rockets, but improvisation saved the day again. All the emergency-planning emphasis had been on dealing with \*foreseeable\* problems; very little attention had been given to building versatility into the system so that \*unforeseen\* difficulties could be handled. One might speculate that this is a "characteristic error" of organizations that try hard to plan for all possible failures.

Henry Spencer at U of Toronto Zoology

#### Computer-generated checks

Art Werschulz <agw@cs.columbia.edu> Tue, 9 May 89 12:25:37 EDT

Yesterday, I received a check from my mother for a substantial amount of money. I took said check to the bank and deposited it, and then asked how long it would be held. I expected an answer of "five days," since the check was from another state.

Much to my surprise, the teller said that there would be no hold at all on the check. You see, it was printed out by Mon's ImageWriter, and hence was a computer-generated check (courtesy of "Dollars and Sense" for the Mac SE, as I recall). The bank's policy was to not put a hold on \*any\* computer-generated checks.

The RISKS of such a policy are mind-boggling. One who desires to commit larceny on a large scale need only acquire an ImageWriter, a Mac, some program that prints out checks, and a supply of checks that can be fed into the printer.

Art Werschulz

#### Hear No Evil (RISKS-8.68)

<microsoft!clayj@uunet.uu.net> Tue May 9 08:57:13 1989

First, as a followup to the article about the movie audio problem reported in Risks 8.68: My understanding of FARs (Federal Aviation Regulations) is that during landings and takeoffs, everything that could conceivably interfere with the safe, rapid evacuation of the A/C has to be stowed. It wasn't noted what sort of A/C the writer was flying in, but, unless it was one of the newer widebodies with ALL of the move screens embedded in the overhead or in some other fashion set up so as to NOT block ANY aisles, lights, etc, then the crew was almost certainly in violation of several FARs. In any case, I think the hazards presented by the continuation of the movie into the landing (people tied to thier seats with headsets, not paying attention to crew instructions, lighting not set full on, headsets preventing people from hearing crew instructions, etc) would FAR outweigh the potential anger from folks who wanted to watch the whole movie. I would suggest that the writer contact the airline, and investigate the possibility of reporting the violation to the FAA.

Clay Jackson, Microsoft

## Computer Bugs/Recalls/Upgrades

<microsoft!clayj@uunet.uu.net>
Tue May 9 08:57:13 1989

I own a HeathKit ID5001 Weather Computer, which is essentially a set of basic weather instrumentation (Pressure, Temp, Humidity, Wind Speed/Dir) controlled by a Z80C. The Z80's programming resides in an EPROM in the unit. One of the "features" of this unit is that it is battery backed, and will continue to record data during a power outage. It also has memories, which contain things like High and Low Temps, Highest Wind Gust, and other goodies. Heath is pitching this unit very hard at Aviation users, and makes a very clear point of noting in their ads and documentation that the unit correctly computes average wind direction/velocity (in compliance with FARs) over a 1 minute interval. Since the unit will potentially be used to provide pilot briefings at small (uncontrolled) airports, I think it's important that the company be forthcoming with any "bug" fixes and/or corrections to their code. Unfortunately, that has not been my experience:

A few weeks ago, I called Heath Technical Support (on a different matter) and asked "by the way, I also have a 5001, have their been any ROM changes since I bought the unit several years ago (I bought one of the first production units)?" The answer was an unqualified "No, there have been no changes since the unit went into production". Last week, I ordered and received the "Technical Manual" for the unit. On about page 5, taking up a whole page, was a listing of the 4 different RELEASED versions of the ROM, and the checksums (there was also a listing for a 5th ROM version, with the notation "Never Shipped"). On the next page was a listing of "Operational Characteristics", one of which was a note that read:

"On battery backed units from the first production run, there was a problem such that after a power failure, the true high wind gust reading is replaced by a random value". It went on to note that this problem was corrected by a later release of the ROM.

To their credit, when I called Heath and reported that I had the problem, they agreed to send my a ROM, at no charge. But, I could NOT get the person I spoke to to tell me what ELSE had changed.

Clay Jackson, Microsoft



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 8: Issue 70

**Friday 12 May 1989** 

## **Contents**

Computers in mathematical proofs

**Henry Spencer** 

- Re: An Atlantis spacecraft computer problem resolved nicely **Yves Deswarte**
- Company sued for "computerized" firing scheme

Emily H. Lonsford

Logged on and Unattended

**NOT FROM Jon Orseck** 

Dot Matrix == valid and LaserReceipts

Mike Albaugh

Computer generated checks

John McLachlan

**Darin McGrew** 

- Auto electronics and Radio Transmitters don't mix!
  - Peter Morgan Lucas
- Mitnick update

Rodney Hoffman

TRW & SSA

Michael J. Tighe

- Centralized Railroad Dispatching **Chuck Weinstock**
- Info on RISKS (comp.risks)

#### Computers in mathematical proofs

<henry@utzoo.UUCP>

Thu, 11 May 89 03:18:49 EDT

The March 1989 Scientific American has a very interesting little piece in its "Science and the Citizen" column, talking about the growing acceptance of computerized proofs in mathematics. It cites the 1976 Haken/Appel proof of the four-color theorem, and the controversy that followed, but observes that at least in principle, that result could be checked by hand. Now we have a significant proof for which hand checking is out of the

question: Clement W.H. Lam of Concordia University has used 3000 hours on a Cray-1, spread over two years, proving an instance of one of Gauss's conjectures ("there are no finite projective planes of order 10", to be precise). This proof, unlike the Haken/Appel one, is meeting little opposition, despite its complexity (100 trillion cases) and the fact that it was done with a collection of small programs rather than a single systematic large one.

Lam himself says he was hoping for a positive result, which would be easy to check, rather than a negative one. But he is fairly confident in his result, citing two reasons: (a) the programs did do some internal consistency checks; (b) the result agrees with "mathematical intuition" (for example, an order-10 projective plane is known to be forbidden to have any symmetry, which apparently is almost unheard-of for such an object).

Mathematicians are coming to accept computers, it seems. Ronald L. Graham of Bell Labs observes that nobody has flatly refused to accept Lam's result, as some did for the Haken/Appel result. Haken himself observes that there is a more mundane explanation for that: many of the objectors were older mathematicians who have since retired.

Haken and Graham both observe that "simple theorems should have simple proofs" is a religious belief rather than a law of nature, and is verifiably false in some simple artificial mathematical systems.

Henry Spencer at U of Toronto Zoology

#### ★ Re: An Atlantis spacecraft computer problem resolved nicely

Yves Deswarte <deswarte@laas.laas.fr> Thu, 11 May 89 12:20:05 -0200

Except if recent major changes have been applied to the space shuttle avionics system, the 5 General Purpose Computers (GPC) are not organized in 2xpairs + 1 back-up, but in a redundant set of 4 computers + 1 back-up. A 2x2 configuration (Stratus-like) would not fulfill the requirement of remaining operational after two non-simultaneous or non-identical faults. With the 4-set configuration, "the first two [GPCs] to fail ... must be identified to the crew as failed; the third should also be identified as failed, but only by achieving as much coverage as is possible within limited processing and storage overhead." (\*) That means that the 4 GPCs tolerate 2 independant faults and have a high probability to tolerate the 3rd fault (the coverage of the built-in test equipment -BITE- is 96.8 %).

This is achieved by voting mechanisms, automatic diagnostics and (manual or automatic) reconfiguration.

The back-up GPC takes control (after manual reconfiguration) only
- if the voting mechanisms are defeated by two simultaneous identical
faults (2 faulty GPCs have identical outputs), or by the 3rd fault

if not covered by the BITE: 3.2% probability,

- or if a software error disbles the 4 main GPCs.
- (\*) "Redundancy Management Technique for Space Shuttle Computers" J.R. Sklaroff, IBM J.Res.Develop., January 1976, pp.20-28
  - -- Yves Deswarte, LAAS-CNRS & INRIA, Toulouse, France -- deswarte@laas.laas.fr

[Yves, Many thanks. I apparently did a mental switch and crossed the A320 with the Shuttle. But in any event, it is my understanding that the shuttles have never had to depend on the backup software. I hope someone will correct me if that is wrong. PGN]

## ✓ Company sued for "computerized" firing scheme

Emily H. Lonsford <m19940@mwvm.mitre.org> Thursday, 11 May 1989 09:21:43 EST

This morning on National Public Radio there was a report on a trial in St. Louis, MO. The juryless trial is a class action suit against the Continental Can Company, which has more than one plant in St. Louis. The company is being sued by a group of more than 200 former employees who allege that a computer program was used to target them for termination before they could reach retirement age, thus denying them their pensions (and presumably saving money for the company.)

The report went on to say that Continental Can was the leading beer-can maker in the sixties, but fell on hard times in the seventies and has had layoffs.

Although the report did not specifically state it, I assume that the laws that pertain here would be those protecting older workers against age discrimination -- not against computerized screening (whether for age or anything else.)

- \* Emily H. Lonsford
- \* MITRE Houston W123 (713) 333-0922

#### Logged on and Unattended

Jon Orseck <orseck@eniac.seas.upenn.edu> Thu, 11 May 89 12:41:14 EDT

I am NOT orseck@eniac. I don't know him.

He was working two shells deep and only logged out the first, leaving the % prompt visible on the screen and a shell exposed.

Just imagine what would have happened had I sent letters apparently from him or posted embarrassing or inflammatory articles to newsgroups such as alt.sex.

Never leave your terminal logged on and unattended!

#### Dot Matrix == valid and LaserChecks

Mike Albaugh <albaugh@dms.UUCP> Fri May 12 13:51:34 1989

This attitude goes back a ways. Around 1980 I almost had to swallow a dinner tab for 20+ people because accounting had a strict rule of no re-imbursement of restaurant tabs without "a cash-register receipt". The fact that the restaurant in question liked to consider itself "high class" and thus only issued hand-written receipts did not impress them. Five minutes work with a dot-matrix printer and a pair of scissors saved me \$300. Had I not been so ethical it could have saved me more...

Mike Albaugh

## computer generated checks

<jmclachlan@lynx.northeastern.edu>
Thu, 11 May 89 09:43:43 EDT

Was the signature also printed by the computer? I would hope not, since anyone who can get at your mother's computer would clear your mother's account.

As for the bank holding a computer generated check, their policy seems strange. Most companies pay employees with computer generated checks. Do the banks treat these checks any different? I'm very curious.

John Mc

[Payroll checks used to be printed on CHECK PRE-SIGNED Stock.

It is even "easier" to laser the whole thing, including the signature.

But then the computer system and the staff had better be trustworthy. PGN]

#### ★ Re: Computer-generated checks (RISKS-8.69)

Darin McGrew <mcgrew@ichthous.Sun.COM>
11 May 89 23:27:58 GMT

Stores that cash payroll and similar checks (very common in many farming communities) are vulnerable to this assumption as well. People who would never take a fake \$500 bill think nothing of taking a fake payroll check.

I read of a ring of payroll check counterfeiters that was caught recently. The (new) assistant manager who was called to approve the check had worked for the company the check was allegedly drawn against, and noticed that it didn't look like the paychecks he'd received. Then he looked more closely and noticed misspellings, incorrect addresses, etc., and called the police.

It manifests itself in a variety of ways, but the basic issue is that computers are making it easier and cheaper to generate documents that look official and genuine.

Darin McGrew mcgrew@Sun.COM

#### Auto electronics and Radio Transmitters don't mix!

"Peter Morgan Lucas, Network Support, Swindon" <PJML@IBMA.NERC-WALLINGFORD.AC.UK> Tue, 09 May 89 16:18:08 BST

Just a note to let you know of a possible risk to all of those of you who drive cars with electronic fuel injection systems.

My father's newly acquired Volvo 480i has an interesting characteristic. When i operate my VHF ham radio gear (100 watts output at 144MHz), the car gives a cough (!) if accelerating hard when i press the transmit switch. The radio signal is clearly getting into the ignition/injection microprocessor and causing some sort of false triggering. The problem is only of very brief duration (approximately a quarter of a second) after which it clears itself. This is only noticeable when accelerating hard in low gears (45MPH in second, 65-70MPH in third). The local Volvo dealer was somewhat perplexed (hes only a salesman, not a RF engineer, after all!) and said he would contact the importers to see if there's any modification (suppressor kit) to get round the fault.

Point is, if 100 watts can cause the effect, is there any risk in driving past other VHF transmitters (TV, FM radio, police, military installations) where the transmitted power may well be 250 kilowatts????

Pete Lucas G6WBJ

#### Mitnick update

Rodney Hoffman <Hoffman.ElSegundo@Xerox.com> 12 May 89 14:58:47 PDT (Friday)

When last we heard about Kevin Mitnick, the hacker once called "as dangerous with a keyboard as a bank robber with a gun," the judge had rejected a plea bargain as too lenient, saying Mitnick deserved more than the agreed one year of jail time. (See <u>RISKS 8.65</u>)

According to a wire service story in the 10 May 89 'Los Angeles Times,' Mitnick has now reached a new agreement, with no agreed-upon prison sentence. He pleaded guilty to stealing a DEC security program and illegal possession of 16 long-distance telephone codes belonging to MCI Telecommunications Corp. The two charges carry a maximum of 15 years and a \$500,000 fine. The government agreed to lift telephone restrictions placed on Mitnick since he was jailed in December.

At DEC's request, Mitnick will help the firm identify and fix holes in its security software to protect itself from other hackers. He will also cooperate in the government's probe of Leonard DiCicco, a fellow hacker. (DiCicco is the 'friend' referred to in RISKS 8.13 who turned Mitnick in.)

[As the old saying goes, with friends like that, who needs enemies. PGN]

#### ✓ TRW & SSA

Michael J. Tighe <mjt@super.org> Fri, 12 May 89 19:02:56 EDT

The credit bureau of TRW has been working with the Social Security Administration to verify its database of 140 million names and Social Security numbers. In order to cover the cost, TRW is paying the Social Security Administration \$1 million, while Social Security Administration will provide a matching \$1 million.

Since the Social Security Administration is asking for a budget increase for their computer and telecommunications systems, several legislators are outraged by the fact they they are spending \$1 million for this non-government project. Claiming that the project is "as far away from the mission of the Social Security Administration as anything I have ever come across", Senator David Pryor (D-Ark) questioned the competence and credibility of Social Security Administration Commissioner Dorcas R. Hardy and asked for an investigation by the HHS inspector general.

In addition, several lawmakers such as Dale Bumpers (D-Ark) believe the project to be a violation of civil liberties. Said Bumpers, "I don't like any public institution releasing an individual's private information." The American Law Division of the Congressional Research Service has already concluded that the project is a violation of the Privacy Act of 1974.

Mike Tighe

#### Centralized Railroad Dispatching

Chuck Weinstock <weinstoc@SEI.CMU.EDU> Tue, 09 May 89 15:51:20 EDT

Railroad Brings Far-Flung Dispatchers Together in Huge Computerized Bunker by Daniel Machalba, Wall Street Journal, May 9, 1989

Starting next month, Union Pacific Railroad train dispatchers will begin working at computers in a windowless bunker built inside an old freight house in Omaha, Neb. The railroad designed the structure's 18-inch-thick, reinforced-concrete walls to withstand, if need be, a telphone pole hurled by a 180-mile-an-hour tornado. The precautions show the importance and risks of railroads' move into centralized, computer-aided train dispatching. By consolidating dispatchers now located at 10 far-flung field offices from Oregon to Omaha, Union Pacific expects to reap savings of more than \$20 million a year. But it must also safeguard its new center from disruptions that could cripple railroad operations on a wide scale. "The bunker will survive anything short of a nuclear attack," says Michael Walsh, chairman of the rail unit of Union Pacific Corp., Bethlehem, PA.

Last March, CSX Corp. opened a similar computerized dispatching center in Jacksonville, FL. The company says the new center will reduce the number of dispatchers needed to run its 20,000 miles of railroad to 350 from 550, while consolidating 34 dispatch offices into one. At the heart of the new center is computer software that can track the progress of trains and automatically switch tracks and signals, so that a fast freight train can pass a slower one. Freed of such routine tasks, dispatchers will be able to concentrate on special situations. Railroad officials say such efficiencies will make it possible for each dispatcher to control double or triple the amount of track. They also hope that bringing the dispatchers into one big room, with panoramic views of trackage projected onto wall screens, will reduce communications problems and resultant train delays.

CSX dispatcher Jan Cato gives one example of how the centers are more efficient. In order for Amtrak's southbound Silver Star to overtake and safely pass two freight trains on its way from Savannah, GA to Jacksonville, she merely types in the locomotive numbers, speeds and other vital data about the trains and the computer does the rest of the work. Previously she had to throw no less than 50 levers manually to line up switches and signals.

"The computer does the thinking when it comes to things such as tonnage, speed, and priority," said Union Pacific dispatcher Bob McKenzie last month in the company's employee magazine. "But it can't determine when you have problems like a train with an engine down, broken air hose or a train down during inspection of a hot-box [overheated axle]. That's when a dispatcher needs to step in."

Some dispatchers worry about information overload. "I have my doubts I could physically handle the expanded territory that would come with the new system," says Richard Pennisi, a Union Pacific dispatcher in Cheyenne, WY., who is taking a cash settlement rather than moving to take a job at the Omaha dispatch center.

Other railroads say they are reluctant to move their dispatchers to a single location, fearing a widening gap between dispatchers and the territories they cover. "We just don't think we can operate the railroad as well without the day-to-day, eye-to-eye contact," says Jack Martin, a senior assistant vice president of Norfolk Southern Corp. However, officials of Burlington Northern Inc.'s rail unit are closely watching the new central facilities. Burlington Northern, which has already cut the number of its dispatch offices in half from 14 a decade ago, is considering further consolidation to one or two locations.

CSX's dispatch center, which is housed in a circular building 150 feet in diameter is permitting the railroad to retire antiquated dispatching facilities such as a 50 year old one in Deshler, Ohio. Dick Fliess, a CSX Transport vice president, says the company has solved software problems that slowed some train operations when the new center opened.

At Union Pacific's dispatch center, which will cost about \$47 million, the railroad is also consolidating its crew-calling staff, previously scattered in four regional centers, into second story offices above the dispatching bunker on the ground floor.

[Someone in the rec.railroad newsgroup pointed out that there is a real risk

of centralizing dispatching beyond the obvious one of a system failure. The UP is likely to be one of the railroads that moves around the MX trains. With centralized dispatching it becomes easier to determine that a particular block of cars always move around together (and thus possibly contain MX's). Furthermore, knocking out the center not only shuts down the railroad, but also disables (or at least impedes) the mobility of the MX. Chuck]



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 8: Issue 71

# Wednesday 17 May 1989

#### Contents

- American Airlines' reservation system crash **Dave Curry**
- NCIC information leads to repeat false arrest suit **Rodney Hoffman**
- Hacking for a competitive edge **Rodney Hoffman**
- Privacy of SSA records Marc Rotenberg
- Info on RISKS (comp.risks)

# American Airlines' reservation system crash

davy@riacs.edu <Dave Curry> Sat, 13 May 89 18:38:13 -0700

Excerpts from "Travel agents in a holding pattern after airline ticket computer stalls", San Jose Mercury News, 5/13/89 (reprinted from N.Y. Times):

"The nation's largest airline computer reservation system, American Airlines' Sabre, inadvertently shut down for almost 12 hours Friday, disrupting the operations of about 14,000 travel agencies nationwide. A large portion of American itself was left without information about who was booked on flights and whether seats were available, and the airline was forced to revert to writing tickets by hand to serve tens of thousands of travelers. American said, however, that there were no major disruptions of its 2,300 daily flights.

The computer shutdown was one of the longest for what has been considered one of the airline industry's most reliable reservation systems. [....] John Hotard, manager of corporate communications for American, said the Sabre system, housed in an underground bunker-like building in Tulsa, OK, failed shortly after midnight Friday while workers at the computer center were installing additional disk drives as part of a system expansion.

Service was not restored until noon Friday, he said. But some travel agencies said their terminals did not resume functioning until one or two hours after that. Apparently, no information about reservations and other travel plans was lost during the failure. [....]

Hotard said the problem with the computer system was a failure in its software. He said the part of the American computer system that handles flight operations -- like crew scheduling, fuel loads and weight loads on American's fleet of airplanes -- was not affected, so flight operations were not disrupted.

[The system has EIGHT IBM 3090-200 E mainframes, designed to survive ordinary hardware malfunctions. This appears to be a software upgrade screwup that downed the whole system. PGN]

### NCIC information leads to repeat false arrest suit

Rodney Hoffman <Hoffman.ElSegundo@Xerox.com> 14 May 89 17:36:59 PDT (Sunday)

An article by James Rainey in the 'Los Angeles Times' 12-May-89 reports that Roberto Perales Hernandez has been jailed twice in the last three years as a suspect in a 1985 Chicago residential burglary. The authorities confused him with another Roberto Hernandez due to a single entry in the FBI's National Crime Information Center computer.

The two Roberto Hernandezes are the same height, about the same weight, have brown hair, brown eyes, tattoos on their left arms, share the same birthday, and report Social Security numbers which differ by only one digit!

The falsely imprisoned man has filed suit charging the Hawthorne (CA) Police Dept., Los Angeles County, and the state with false imprisonment, infliction of emotional distress, and civil rights violations stemming from the most recent arrest last year. He had previously received a \$7,000 settlement from the county for holding him 12 days in 1986 before realizing he was the wrong man. In the latest incident, he was held for seven days then freed with no explanation.

#### Hacking for a competitive edge

Rodney Hoffman <Hoffman.ElSegundo@Xerox.com> 14 May 89 17:39:06 PDT (Sunday)

From the 'Los Angeles Times' 12-May-89:

Two former Tampa, FL TV news managers have been charged with illegally tapping into phone lines and computers at another station to gain a news edge over their competitors. Former new director Terry Cole and assistant news director Michael Shapiro at WTSP-TV have been charged with 17 counts of computer hacking and conspiracy in the theft of information from WTVT-TV through computer phone lines, authorities said. Their arraignment is set for May 19. If convicted, each could face a maximum prison sentence of 85 years. The two were fired from WTSP when the station learned of the alleged thefts. The break-ins

began in November but were not noticed until Jan. 12, when WTVT's morning news producer noticed that files were missing, authorities said. Computer experts determined that an intruder had rifled the files. Authorities said Spapiro knew WTVT's security system thoroughly because he had helped set it up while working there as an assignment manager befroe being hired away from WTVT in October.

I have no idea what sort of charge "17 counts of computer hacking and conspiracy in the theft of information" really is.

# ✓ Privacy of SSA records (update on RISKS-8.70)

<mrotenberg@cdp.uucp>
Sat, 13 May 89 11:11:49 -0700

Two clarifications regarding the item in <u>RISKS-8.70</u> on the record exchange involving the Social Security Administration and TRW:

- The proposed transfer of the social security records to TRW came to an end after the plan was disclosed at an April hearing of the Senate Committee on Aging.
- The primary concern expressed by members of Congress was the privacy violation, not the cost to SSA. Senator Pryor said that he was glad the SSA had "seen fit to preserve the confidentiality of the Social Security files. Unfortunately," he said, "this action comes to late to protect some 150,000 people whose files were violated in a test run conducted for TRW [in 1987] and for more than 3 million people on whom verifications were conducted for Citibank and other firms in past years." The HHS Inspector General also described these activities as "the largest breach of privacy in the history of the program."

As a matter of privacy law, the plan violated a general provision in the 1974 Privacy Act which states that no agency should disclose any record unless it obtains the consent of the record subject or a particular exemption applies. (None applied in this case).

Some attorneys within SSA were not convinced that the language in the Privacy Act was dispositive, but a decision of the Supreme Court a month before the Senate hearing affirming the privacy of computerized criminal records stored by the federal government tipped the balance in favor of stopping the program.

- Marc Rotenberg



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 8: Issue 72

**Sunday 21 May 1989** 

# Contents

- Air Force Bombs Georgia
  - henry cox
- The Geomagnetic Storm of 13 March 1989
  - **Brian Randell**
- Tolerability of Risk
  - **Martyn Thomas**
- More magnetic stripe woes
  - Joe Morris
- Dive Computers revisited
  - **Henry Cox**
- Info on RISKS (comp.risks)

### Air Force Bombs Georgia

henry cox <cox@rand.ee.mcgill.ca> Thu, 18 May 89 10:49:24 EDT

[ From the Montreal Gazette, 12 May 1989]

US AIR FORCE PROBES WHETHER TRANSMITTERS CAUSED BOMB TO DROP

Atlanta - US Air Force investigators are examining whether electromagnetic radiation from military transmitters may have caused an F-16 jet to accidentally drop a bomb on rural West Georgia last week, and Air Force official said yesterday.

The possibility of electromagnetic interference, however, is only one of several potential causes the Air Force and Army is investigating, said Dee Tait, an official at Moody Air Force Base where the F-16 is stationed. A final accident report won't be ready for 30 to 90 days, she said.

No one was injured in the May 4 explosion, but the 230 kilogram bomb ripped through a wooded area and has prompted a Georgia congressman to call for a review of Air Force flight procedures state wide.

According to forces officials, the inadvertent bombing occurred when one of four armed jets from the 247th Tactical Fighter Wing at Moody was training last Thursday over Fort Benning's "Kilo Impact Area" in Muscogee County.

The pilot of the plane, who has not been identified, tried to release a bomb over the practice range, but it would not drop. As the pilot circled back over Marion County, the bomb fell and its 90 kg of explosives shook windows of houses 900 metres away.

[ Short explanation of EMI causes deleted ]

It [EMI] has been attributed to navigation problems with the Army's UH-60 "Black Hawk" Helicopter, which has been banned from flying near 100 transmitters worldwide.

In the case of the F-16, high levels of electromagnetic radiation can accidentally detonate electro-explosive devices, or EEDs, that release bombs, missiles and fuel tanks from the underside of the plane, according to an Air Force {\it Explosive Safety Standards} manual obtained by the Macon {\it Telegraph and News}.

The vulnerability of Air Force planes with EEDs has become and issue at Robins Air Force Base near Warner Robins, Ga., where the Air Force has been shutting down part of the high-powered PAVE PAWS radar station every time and EED-equipped plane lands at the base.

The Air Force operates four PAVE PAWS facilities, which use radar powerful enough to probe objects in space. A current study at the Robins base is examining the power of the pulsed radar beams from PAVE PAWS and whether it disrupts ultra-sensitive electronic equipment on aircraft.

The partial shutdowns preceded a March 1988 Air Force report that stated "the high power contained in PAVE PAWS pulses may pose a danger to elecro-explosive devices carried on military and commercial aircraft."

Tait confirmed that the F-16 [involved in the incident ] had been equipped with EEDs, tiny explosive charges that release the shackles that hold the bomb onto the jet. "They are looking into that," she said. However, she added, "the bomb-release mechanisms on F-16s are designed to preclude electromagnetic interference."

Henry Cox (cox@pike.ee.mcgill.ca)

#### ★ The Geomagnetic Storm of 13 March 1989

Brian Randell <Brian.Randell@newcastle.ac.uk> Tue, 9 May 89 18:51:04 BST A colleague drew my attention to an article in Radio Communication (Vol. 65, No. 5, May 1989), which made me realise belatedly just how vulnerable we are to the effects of magnetic storms. Below I excerpt from the article, without permission.

#### THE GEOMAGNETIC STORM OF 13 MARCH 1989

Ted Harris and David Kerridge, Geomagnetism Group, British Geological Survey, 29 March 1989.

"The largest magnetic storm for 40 years started at 2am on 13 March 1989... The intensity of the storm was such that the aurora borealis (northern lights), normally restricted to high latitudes, was seen clearly in the south of England, and there were reports of observations of the aurora in Italy and as far south as Jamaica.

"The rapid changes in the geomagnetic field during the storm induced voltages in power lines, transoceanic cables, and telephone and cable TV networks. In Quebec, transformers in the Canadian electricity supply tripped, blacking out large areas of the Province and plunging more than a million people into darkness. (No doubt with a consequential blip in the birth-rate in nine months time!)

"Ionospheric disturbances caused disruption of radio communications and resulted in the loss of TV reception in some areas. Satellite communications were also affected - as were satellite orbits as the increased ionospheric density produced extra drag.

"The increased radiation at high level created such potential hazards that a Concorde airliner on a transatlantic route took a more southerly flight path to avoid subjecting its passengers to radiation. Astronauts aboard the the space shuttle 'Discovery' would have been prevented from working outside the space craft because of the danger. The shuttle mission was recalled a day earlier than planned because of computer malfunctions which could have been caused by the storm.

"At sea-level, North Sea exploration companies reported that `down-well' instruments, used to steer drill heads, had experienced violent swings in compass readings of up to 12 degrees! A Norwegian geophysical exploration company reported that all surveying has been halted after receiving warnings of the storm and its severity from GRG. The director of operations reported that two navigation systems used to fix the position of survey ships, which were in agreement prior to the storm, were now diverging. GPS (Global positioning system) satellites experienced increased drag which retarded their orbits so much that positional accuracy at the Earth's surface was lost. ...

"Solar activity is likely to peak during 1990 (Solar Maximum), resulting in more magnetic storms and a generally high level of magnetic activity over the next two years at least."

Brian Randell, Computing Laboratory, University of Newcastle upon Tyne

#### ★ Tolerability of Risk

Martyn Thomas <mct@praxis.UUCP> Wed, 17 May 89 14:55:43 BST

I strongly recommend the publication The Tolerability of Risk from Nuclear Power Stations, Health and Safety Executive, Her Majesty's Stationery Office, December 1987. It contains a thorough discussion of the way in which society perceives, and tolerates, risks from different sources. It also contains interesting UK actuarial statistics (...in Britain, a man of 20 has roughly a 1 in 1000 chance of dying in a year, for a man of 40 it is 1 in 500, at sixty, it is 1 in 50 for a man, 1 in 100 for a woman ...).

There is a companion volume of comments received from trade and professional groups.

--

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK. Tel: +44-225-444700. Email: ...!uunet!mcvax!ukc!praxis!mct

#### More magnetic stripe woes

jcmorris@mitre.arpa <Joe Morris> Fri, 19 May 89 09:21:12 EDT

Quick background: the Washington area Metro subway system uses fare cards with a magnetic strip on the back. You buy a card of some particular value; it is debited as it is used (the fares are distance-sensitive) and each time you exit Metro the remaining value is recorded \*and printed\* on the farecard. With this in mind, the following news article appeared in the 19 May issue of the \_Washington\_Post\_, p. C7 (as usual, without permission):

DASH Magnets and Farecards: A Fatal Attraction

Alexandria's DASH bus system [a suburban transit system] thought it was promoting public transit Wednesday when it gave riders 2,500 refrigerator magnets in honor of national "Transit Appreciation Day."

Funny thing, though, how the magnets apparently erased the value of an unknown number of riders' Metro Farecards, officials said yesterday.

"We didn't do it intentionally, and definitely apologize to our passengers for any inconvenience," said DASH General Manager Sandy Modell.

Metro officials said riders can obtain new cards by mailing the now useless ones to Metro's treasurer's office [...].

The number of Farecards affected and the potential amount owed riders was not known yesterday, DASH and Metro officials said.

The value of a Metro Farecard is magnetically encoded when the card is purchased. Cards are scanned electronically when passengers pass them through the fare gates, which automatically deduct the trip fare.

Apparently, the small thin magnets, which fit in wallets and change purses, erased the Farecards when they were stored together, said Metro spokeswoman Beverly Silverberg.

"It happens all the time" when women carry purses with magnetic clasps or riders carry other types of magnets, Silverberg said. Modell warned that magnets can have the same effect on automated teller machine cards and some credit cards.

DASH bought the magnets, which included the DASH telephone number, from the American Public Transit Association, which offered them to transit agencies across the country, Modell said. She did not know if any other systems were similarly affected.

DASH passed out the magnets "as a token of appreciation" to riders, Modell said.

### Dive Computers revisited

henry cox <cox@rand.ee.mcgill.ca> Thu, 18 May 89 10:48:02 EDT

Some time ago several submissions dealing with the potential risks of dive computers (which automatically monitor the nitrogen level in the divers blood, and tell him when he must surface, etc.) appeared in RISKS. Since then, I acquired one myself. My experience might be of interest to others.

Soon after Christmas, two friends and I purchased three Oceanic Datamaster II (a particular brand) dive computers. At the same time, we also purchased "Slimline" compasses, which were designed to fit into the same console. All of the units (three of three) were eventually returned due to defects:

- 1) Due to electromagnetic interference, when the computer was ON, the compass would point in whichever direction the console pointed making completely useless.
- 2) One unit was broken when shipped (or was broken during shipping), and never worked at all.
- 3) Among other features, the computer was supposed to report the "dive time remaining", based on air consumption and no-decompression nitrogen levels whichever is less. On one unit, this was not recomputed correctly stuck on 29 minutes, even when there was no air left in the tank it was connected to. (Yep, I'll just sit here and hold my breath for 29 minutes...)
- 4) The last unit appeared to work correctly when checked out in the pool, but failed completely on its first real dive, giving no readings at all.

All three units were returned and replaced with and upgraded model, the Datamaster Sport - all three of which have worked properly to date. The EMI problem was fixed with a redesigned console boot, which moved the compass further away from the computer.

Certainly, some of these problems should have been caught and corrected by the manufacturer (Oceanic USA, inc.) - particularly the EMI interference on the compass, which would have been obvious to anyone who turned the unit on and tried to use it. The other problems MAY have been caused by shipping, although I doubt it, as the cartons arrived undamaged. In any case, presumably the unit will be subjected to some rough handling during use, and should be designed handle it.

I think that the real problem here was improper and incomplete testing of the product before it was shipped out the door - potentially, a VERY serious RISK, given the nature of the activity is designed for.

As has been stated many times before, computer readouts are no excuse to turn off your brain, and it is not wise to rely on any one instrument. In my case, I dive with two complete sets of gauges (my old set plus my dive computer), and I continue to work out nitrogen levels for myself. Doing otherwise would be very foolish.

Henry Cox

DISCLAIMER: I have NO CONNECTION whatsoever with OCEANIC USA or any other dive equipment manufacturer (except that I own some of their equipment). The opinions stated above are my own. The events which inspired them are also mine (unfortunately).



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 8: Issue 73

**Monday 22 May 1989** 

#### Contents

State computer system scrapped

**Bruce Forstall** 

Fax Attack

**Chuck Dunlop** 

Client responsibility for organization's head crash

David A Honig

Re: Computers in mathematical proofs

Robert Lee Wilson Jr

**Robert English** 

**Travis Lee Winfrey** 

Formal Methods -- Call For Papers

**Nancy Leveson** 

Info on RISKS (comp.risks)

# State computer system scrapped

Bruce Forstall <forstall@june.cs.washington.edu> Mon, 22 May 89 12:20:11 PDT

(Reprinted WITH permission of The Seattle Times, Friday, May 19, 1989, p. B1)

State bytes off more than it can chew DSHS to scrap computer system by Jim Simon, Times Olympia bureau

OLYMPIA -- After the state spent \$20 million and nearly seven years trying to computerize its public-assistance program, the first caseworkers to use the so-called COSMOS system made their own discovery: They could figure out a client's benefits faster by hand than with the computer.

The Department of Social and Health Services announced yesterday it was swallowing its losses and terminating COSMOS, considered the most expensive, and some say ill-advised, computerization effort ever undertaken by the state.

"The project needed to be stopped and we stopped COSMOS," said DSHS Secretary Richard Thompson, the fifth agency head who has wrestled with the system. "There's a lot of things that went wrong that we still have to look at. My concern was that we had to stop spending the money."

The state has so far spent about \$4.1 million and federal agencies about \$15.2 million on COSMOS--the Community Services Management and Operations System. Thompson said DSHS ultimately may be liable for up to \$4 million of the federal share.

A consultant's report released earlier this week recommended scuttling COSMOS. The report cited poor management, an overly complex design, difficulty to use by caseworkers and the use of untested software.

Proponents originally predicted the troubled system would save the state money by allowing computers rather than caseworkers to calculate eligibility for welfare, food stamps and medical assistance.

COSMOS, designed by Pennsylvania-based UNISYS Corp., was thought so advanced that Gov. Booth Gardner and some of the state's computer professionals likened it to ``artificial intelligence."

But its complexity apparently kept it from working at all.

That became obvious this year when the system was installed on a pilot basis in the Longview and Vancouver DSHS offices, according to Thompson and others.

Workers there found it took up to twice as long to figure out a client's eligibility from COSMOS as it did manually. Using the computer resulted in frequent errors in simple calculations, and perhaps most nerve-wracking for caseworkers, the screen often went blank for long intervals.

"This was an effort to create artificial intelligence so the computer could 'think' about eligibility," Gardner said yesterday. "I don't think we'll mess with artificial intelligence again."

But critics say DSHS had plenty of advance warning about just how high a risk COSMOS represented.

In 1982, when planning first began, the agency estimated it would cost \$10 million and be completed in 1985.

But the agency later sought a more ambitious system that was to cost \$22 million and be completed by the end of mid-1987. Before killing COSMOS, the most recent estimates were that it would cost \$38 million and take until late 1990 to finish.

Gerald Reilly, who headed the DSHS division of income assistance until recently, said the agency decided to keep pressing on until they could test COSMOS in the field.

``We believed you couldn't know how this would work until you took it that far," Reilly said.

Reilly and others acknowledge that the state was aware of problems UNISYS had setting up similar systems for other states.

"But virtually all these big systems have troubles," Reilly said. "The welfare programs themselves are very complex."

"Killing COSMOS was a gutsy move by Thompson," said Rep. Gary Locke, chairman of the House Appropriations Committee. "There's going to be a lot of finger-pointing but there was no sense chasing the good money after the bad."

The death of COSMOS could prove an embarrassment for UNISYS, which has already been paid about \$4.7 million. Two sources said the state attorney general's office is considering legal action. The attorney general's office declined to comment.

A spokesman for UNISYS' local office also would not comment.

Thompson said the agency will still pursue a system to computerize its benefit programs. But the next effort will probably use one of the 17 systems

certified by the federal government using technology that has been tested in other states, he said.

Another major state computer project that has cost taxpayers \$17 million is expected to be scrapped next year. State officials have said they expect to cancel the project to transfer district-court records because it doesn't perform anywhere near the number of tasks court officials expected it would.

#### Fax Attack

<Chuck\_Dunlop@ub.cc.umich.edu> Sat, 13 May 89 12:29:28 EDT

Governor's try to ban unsolicited ads backfires (The Ann Arbor News, 5/13/89)

HARTFORD, Conn - The great fax attack of 1989 -- an all-out lobbying campaign against a bill banning unsolicited facsimile advertising -- may have backfired when the governor's fax machine was jammed for hours with unwanted messages.

Starting Thursday and continuing Friday, Gov. William A. O'Neill's fax machine has been beeping constantly, spitting out unwanted messages from angry businesses that advertise by fax.

The businesses oppose a bill now awaiting O'Neill's signature that would prohibit them from marketing their products by fax without first obtaining the permission of the recipient. Violators would face a \$200 fine.

Starting Thursday morning, dozens of Connecticut businesses faxed to O'Neill's office a form letter arguing against the fax ban.

The stream of fax messages was so constant -- 40 came in before 10 a.m.

-- that the governor's office turned off the fax machine Thursday.

O'Neill's press secretary, Jon. L. Sandberg, said the governor still hasn't decided whether he will sign the bill. But aides to the governor said the persistent lobbying campaign proved how annoying unwanted messages casn be. The inconvenience was compounded because the governor's office was unable to use its fax machine to receive information about spring flooding around the state.

## Client responsibility for organization's head crash

David A Honig <honig@BONNIE.ICS.UCI.EDU> Wed, 17 May 89 09:22:49 -0700

I recently was sent a bill (\$70) for two "lost books" from the campus's (U.C. Irvine) main library. Since I knew I had returned them, I went to check the shelves. I found one of them; I didn't have time to search for the other. When I inquired as to why I had been falsely charged and billed, I was told by the checkout clerk that it was a "computer error". Upon phoning the library, I found that the day I had returned the books the library had had a head crash.

The library policy is to search for "lost" books if the charge is contested, but if they are not found, I am assumed guilty. (What if the reshelvers erred?) There is essentially no recourse; I understand that the Ombudsman

would be impotent. Worse, I am told that this occurs occasionally to others, head crash or not.

What I find remarkable is that this organization would not give the client the benefit of the doubt when they are \*aware of an internal problem\*. Besides this, I wonder about the tradeoffs they made in designing a book-return system so vulnerable to the failure of one of its components (disk drive or human book checker). Are redundant drives or paper records so expensive that a major library cannot use them? I suspect the adminstrators who specified the existing system did not understand what they were doing. I suppose I should not be surprised.

### ✓ Re: Computers in mathematical proofs

Robert Lee Wilson Jr <bobw@ford-wdl44>
Tue, 16 May 89 10:24:27 PDT

While "dying off" of some of the mathematicians who found the computerized 4-color proof intolerable is certainly part of the reason that the computerized "no projective plane of order 10" proof is being accepted, I think there is another significant difference. I knew several mathematicians who had "gone out on a limb" with statements that 4 colors would not suffice, no matter what the predominant belief. I can recall one whose entire career and psyche were devoted to finding non-4-colorable maps. He would literally give new graduate students maps to color, hoping to find one which seemed to require 5 colors. Of course each one got colored with 4 colors, but his faith did not waver.

I have not seen this fervor in regard to the planes of order 10. I have seen papers which included theorems of the form "If there is a projective plane of order 10 then ....", but frequently they also included "If there does NOT exist ..." theorems as well.

The point I am trying to make is more or less this: It is all well and good to give "objective" arguments about why computer proofs are valid or are not, but somehow those arguments wind up supporting what the speaker wanted to believe anyway!

**Bob Wilson** 

#### Re: Computers in mathematical proofs

Robert English <renglish%hpda@hp-sde.sde.hp.com> Wed, 17 May 89 10:21:21 pdt

I don't really see that much difference between a computerized proof and standard proof. In both cases, all steps of the proof must be rigorous. In a computerized proof, the mathematician must rigorously prove that his program is correct. In effect, the program definition becomes a lemma within the larger proof.

Philosophical problems don't crop up until you ask whether the computer

operated correctly, or whether defects in the underlying software (such as the compiler or the operating system) corrupted the results. Since the entire system does not admit rigorous examination, some claim that the process is fundamentally different than rigorous proof.

What this argument overlooks is that rigor does not guarantee correctness to any greater degree than can be achieved in a computer-aided proof. A complicated proof can have errors at many stages, and reviewers cannot be trusted to find them all, any more than programmers can be trusted to find all of the bugs in a complicated computer system. Furthermore, while program proofs do not admit direct human verification, they do allow independent verification by other humans using similar, but different, tools.

The question of whether independent verification actually takes place for program proofs is equivalent to the question of whether each step in a rigorous proof is really verified by independent auditors. In both cases, theoretical verification is possible, but in practice, it may not take place, or the auditing process may fail.

--bob--

## Re: Computers in mathematical proofs

Travis Lee Winfrey <travis@douglass.cs.columbia.edu> Mon, 15 May 89 15:35:22 EDT

>Lam himself says he was hoping for a positive result, which would be easy
>to check, rather than a negative one. But he is fairly confident in his
>result, citing two reasons: (a) the programs did do some internal
>consistency checks; (b) the result agrees with "mathematical intuition"
>(for example, an order-10 projective plane is known to be forbidden to
>have any symmetry, which apparently is almost unheard-of for such an object).

Is anyone more familiar with this work, such as any testing or proving techniques he attempted on his program? 100 trillion bug-free executions seems rather high, particularly given the binary nature of the answer he needed. Has the Lam proof been published yet?

#### Formal Methods -- Call For Papers

<leveson@LCS.MIT.EDU>
Thu, 11 May 89 16:43:21 -0400

Given the forthcoming MoD standard in Great Britain requiring the use of formal methods on safety-critical software, we thought the following might be of interest to Risks readers.

Call for Papers for Special Issues of IEEE Software, Computer, Transactions on Software Engineering:

Formal Methods for Software Engineering

Formal Methods are design and construction methods explicitly based on well-defined mathematical formalisms. Examples are: VDM, Z, box-structures, traces, predicate transformers, state transition systems, axiomatic data types, and many more. These methods promise (1) better control over the system development process through clarity and precision of specification and then of development steps and (2) reduced error commission and persistence through rigor, systematic review, and formal analysis. Much progress has been made in using formal methods, developing support systems for them, and evaluating their applicability on industrially-oriented problems. Applications to critical systems are appearing world-wide, and there is now some commercial interest based on advances in verifiable execution environments. Several standards groups are using formal methods and one - VDM - is undergoing the international standards process.

A coordinated set of papers is planned for September 1990 with a survey plus a tutorial in IEEE Computer, application case studies in IEEE Software, and research papers in IEEE Transactions on Software Engineering.

Oct. 1, 1989 Drafts Due (earlier submissions welcome)
Mar. 1, 1990 Reviews Completed
May 1, 1990 Revisions Completed
September, 1990 Publication

A complete call for papers containing detailed information about submission and content will be published in SEN (July) and each of the journals. Information and a copy of the complete call for papers is available from the editors:

Applications, tutorial, survey: Research Contributions:

Susan Gerhart Nancy Leveson

MCC Software Technology Program Info. & Computer Science Dept.

3500 W. Balcones Dr. University of California Austin TX 78759, U.S.A. Irvine, CA 92717 Phone: 512-338-3492 Phone: 714-856-5517 Fax: 512-338-3899 Fax: 714-856-4056

e-mail: gerhart@mcc.com e-mail: nancy@ics.uci.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 8: Issue 74

Friday 26 May 1989

# Contents

- Aegis, Vincennes, and the Iranian Airbus **PGN** interpreting Matt Jaffe
- Anti-lock brake system failure fail-safe? Jay Elinsky
- Pleasure boat database helps thieves **Howard Gayle**
- SAGE-BOMARC risks

Les Earnest

- SABRE disaster caused by "core corruption" **Andrew Birner**
- Computer Intrusion Network in Detroit Dave Curry
- Robert T. Morris suspended from Cornell **Dave Curry**
- Info on RISKS (comp.risks)

#### ★ Aegis, Vincennes, and the Iranian Airbus (report on a Matt Jaffe talk)

Peter Neumann < neumann@csl.sri.com> Fri, 26 May 1989 13:44:01 PDT

In a keynote talk for the 5th International Workshop on Software Specification and Design in Pittsburgh, 20-21 May 1989, I cited the case of the Aegis' role in the Vincennes' shootdown of an Iranian Airbus as an example of a system in which the design of the user interface was critical.

Matt Jaffe (Jaffe@ics.uci.edu) responded with some comments on the Aegis user interface -- in whose design he had played a part while at RCA -- after which he was invited to gave an impromptu talk on his experience to the workshop.

As you may recall, the Iranian Airbus was shot down by the Vincennes, although it was on schedule, on course, and apparently flying completely normally. There was confusion between the commercial plane being tracked and an observed IFF (Identification, Friend or Foe) squawk from a fighter plane. The altitude

information (Z) was not displayed on the main screens, but only in one of various subtables that had to be called up on a smaller screen. There was no indication of rate of change of altitude (Z', or "Z-dot"), not even a ternary choice among ascending, cruising, or descending. Matt took the view that the user interface could not have done much differently, because of intrinsic limitations on

- 1. the reliability and/or accuracy of the underlying data,
- 2. the physical and logical characteristics of the display devices (alphanumeric raster-scan screens with limited space)
- 3. and the ability of human operators to interpret marginal data in the high volume and high stress environment.

This is an attempt to summarize Matt's main points:

Mode II codes (military use only) cannot be conclusive in determining friend or foe because they can be spoofed by a non-friendly aircraft, as can the civilian use Modes I and III. In this particular case, the military aircraft supplied by the US to Iran almost certainly included Mode II transponders. Note some subtle points here. IFF is to determine the identity of friendly aircraft, not the military capability of a non-friend. In this tragedy, the problem was not in discriminating between friends and all others but between an Iranian F-14 and an Iranian airliner. The identification as Iranian was correct (and presumably not based on IFF but on point of origin). A classification of a Mode II code as belonging to an Iranian military aircraft would seem reasonable given that the airfield from which the aircraft departed was a joint use airport (both civilian and military). What may have happened was that the airliner taxied near enough to an F-14 on the ground as to preclude the system from recognizing that there were in fact TWO aircraft. (ANY sensor has some resolution limits.) Once the airliner was airborne, its lack of further mode II activity would not preclude the display of the old Mode II code. Aircraft may fail to respond to an IFF interrogation (of any code) for a variety of reasons and yet operators (both civil and military) want to have the last recieved code remain displayed.

Thus the entire mechanism contains potential ambiguities. Providing a recency field for Mode II squawks would probably have been a good idea, display space and operator cognitive limits permitting. (At that time and to date, Matt indicated that he knew of no system that provided the age of last squawk; nor did the Navy mention the possibility. Scary?)

The altitude readings are generally unreliable. Thus, the Z' calculations -- irrespective of how they were done -- would be suspect, and subject to possible misinterpretation. Nevertheless, some crude up-down-same field might have been useful.

Uncertain or unreliable information will always be a major problem in any safety-critical system.

From the Navy's point of view, the Captain of the Vincennes did the right thing -- based on what he knew.

No standard Navy shipborad systems could have done the discrimination

automatically. No equipment necessary for the Vincennes mission could have prevented a manual decision from being difficult, nerve-wracking, and error-prone.

The situation was basically untenable in the first place, with hostile aircraft and commercial airliners closely interwoven within an area of great unrest.

[The Stark Captain had said earlier that they had not realized the limitations of the combat system in that kind of an environment. PGN]

Matt made the appropriate disclaimers -- that his knowledge is not current, that his opinions were his own, etc. And his audience was generally impressed with the care with which he had thought out the issues. All in all, this case is of great importance, and bears close consideration. There are many lessons to be learned, some technological and some nontechnological -- many of the latter relating to the intrinsic limitations of trusting the technology, especially under adverse circumstances. PGN

#### Anti-lock brake system failure - fail-safe?

"Jay Elinsky" <ELINSKY@YKTVMT.BITNET> Thu, 25 May 89 07:40:57 EDT

The June 1989 issue of Consumer Reports includes a test of the Chevrolet S-10, as well as three other sport/utility vehicles. The Chevrolet has rear-wheel anti-lock brakes. This is from the "Reliability" section of the report on the Chevrolet:

"The most disquieting [sample defect] was a defective antilock brake controller. At just over 200 miles, the brake warning light came on and the pedal sank almost to the floor. The pedal felt spongy and sank slowly during each brake application. The controller was replaced under the warranty."

I would have expected that a controller failure would leave you with normal brakes, and perhaps a warning light glaring at you to warn that the brakes are now manually controlled. Instead the failure mode sounds like a plain old brake system leak, except that Consumer Reports didn't say that braking power was actually lost. Was there braking power left only because the front brakes, which I understand do most of the braking, weren't controlled by the defective controller? In any event, finding the brake pedal much lower than you expect it to be, is a risk in itself.

It's also interesting that Consumer Reports didn't make a big deal out of this problem, so perhaps they don't consider it to be a major risk.

Jay Elinsky, IBM T.J. Watson Research Center, Yorktown Heights, NY

#### Pleasure boat database helps thieves

Howard Gayle <howard@dahlbeck.ericsson.se> Wed, 24 May 89 14:02:07 +0200

This is based on an article in the Stockholm newspaper Dagens Nyheter, 24 May 1989, p.6. Last year, a law went into effect in Sweden requiring the registration of most pleasure boats. The database is financed by a small "user fee," i.e., a tax. The data are public information. A thief who steals a boat can phone the registration office, tell them the boat's registration number, and obtain the legal owner's name, address, and national ID number. This makes it easy for the thief to impersonate the legal owner when selling the stolen boat.

#### **✗ SAGE-BOMARC risks**

Les Earnest <LES@SAIL.Stanford.EDU>
23 May 89 0131 PDT

This is an account of two ancient (30-year old) computer risks that were not publicly disclosed for the usual reasons. It involves an air defense system called SAGE and a ground-to-air missile called BOMARC.

SAGE was developed by MIT in the late '50s with Air Force sponsorship to counter the threat of a manned bomber attack by you-know-who. It was also designed to counter the political threat of a competing system called Nike that was being developed by the Army.

SAGE was the first large real time computer system. "Large" was certainly the operative term -- it had a duplexed vacuum tube computer that covered an area about the size of a football field and a comparably sized air conditioning system to take away the enormous heat load. It used an advanced memory technology that had just been invented, namely magnetic core, and had a larger main memory than any earlier computers, though it is not impessive by current standards -- it would now be called 256k bytes, though no one had heard of a byte then.

The system collected digitized radar information from multiple sites and used it to automatically track aircraft and guide interceptors. SAGE was designed to work initially with manned interceptors such as the F-102, F-104, and F-106 and used a radio datalink to transmit guidance commands to these aircraft. It was later modified to work with the BOMARC missile.

Each computer site had about 50 display consoles that allowed the operators to assign weapons to targets and monitor progress. As I recall, there were eventually between one and two dozen SAGE systems built in various parts of the U.S.

BOMARC missiles used a rocket booster to get airborne and a ramjet to cruise at high altitude to the vicinity of its target. It was then used its doppler radar to locate the target more accurately so that it could dive at it and detonate. It could carry either a high explosive or a nuclear warhead.

BOMARCs were housed in hardened structures. When a given missile received a launch command from SAGE, sent via land lines, the roof would roll back, the missile would erect, and if it had received a complete set of initial guidance commands in the meantime it would launch in the specified direction.

# Testing the fire-up decoder

It was clearly important to ensure that the electronic guidance system in the missile was working properly, so the Boeing engineers who designed the launch control system included a test feature that would generate a set of synthetic launch commands so that the missile electronics could be monitored for correct operation. When in test mode, of course, the normal sequence of erecting and launching the missile was suppressed.

I worked on SAGE during 1956-60 and one of our responsibilities was to integrate BOMARC into that system. This led us to review the handling of launch commands in various parts of the system. In the course of this review, one of our engineers noticed a rather serious defect -- if the launch command system was tested, the missile would be in a state of readiness for launch. If the "test" switch was then returned to "operate" without individually resetting the control systems in each missile that had been tested, they would all immediately erect and launch!

Needless to say, that "feature" was modified rather soon after we mentioned it to Boeing.

#### Duplexed for reliability

For some reason, I got assigned the responsibility for securing approval to put nuclear warheads on the second-generation BOMARCs, which involved "proving" to a government board that the probability of accidentally launching a missile on any given day as a result of equipment malfunctions was less than a certain very small number and that one berserk person couldn't do it by himself. We did eventually convince them that it was adequately safe, but in the course of our studies we uncovered a scary problem.

The SAGE system used land lines to transmit launch commands to the missile site and these lines were duplexed for reliability. Each of the two lines followed a different geographic route so that they would be less likely to be taken out by a single blast or malfunction. There was a black box at the missile site that could detect when the primary line went bad and automatically switched to the alternate. On examination, we discovered that if both lines were bad at the same time, the system would remain connected to the alternate line and the amplifiers would then pick up and amplify whatever noise was there and interpret it as a stream of random bits.

We then did a Markov analysis to determine the expected time that it would take for a random bit stream to generate something that looked like a "fire" command for one of the missiles. We found that expected value was a little over 2 minutes. When such a command was received, of course, the missile would erect and prepare to launch. However, unless the missile also received a number of other commands during the launch window, it would automatically abort. Fortunately, we were able to show that getting a complete set of acceptable guidance commands within this time was extremely improbable, so this failure

mode did not present a nuclear safety threat.

The official name of the first BOMARC model was IM-99A, so I wrote a report about this problem titled "Inadvertent erection of the IM-99A." While that title raised a few eyebrows, the report was destined to get even more attention than I expected. Its prediction came true a couple of weeks after it was released -- both phone lines went bad on a BOMARC site in Maryland, near Washington D.C., causing a missi

# ✓ SABRE disaster caused by "core corruption"

Andrew Birner <Andrew-Birner%ZENITH.CP6%LADC@BCO-MULTICS.HBI.HONEYWELL.COM> Wed, 24 May 89 18:08 PDT

According to an article by Margie Semilof, entitled "SABRE Recovers from Network Crash", in Communications Week, May 22, 1989, the recent SABRE outage occurred when the "Online DASD formatter was changed erroneously by another software program operating at the same time. This 'core corruption' resulted in the destruction of critical system data on SABRE's 1,800 DASDs."

The article later quotes Jim Juracek, vice president of systems engineering for SABRE Computer Services:

"All the predictable things are covered," Juracek said. "The unpredictable things, such as when a software program gets clobbered by another program . . . [ellipsis hers] there is no way to work with this."

The article further notes that "SABRE is developing software that will provide memory protection of applications, and thereby help prevent against core corruption. That software will not be ready[,] however, until the early to mid 1990s".

Using software for memory protection? In the 1990s? How, I wonder, will they protect their protection software ("quis custodiet ipsos custodes", as always)? Is SABRE is too tightly coupled to its hardware to be moved to a platform that provides hardware memory protection? Or is it just plain too big to be ported?

Andrew E. Birner -- Zenith Electronics Corp -- Zenith/A\_Birner@ladc.bull.com

# Computer Intrusion Network in Detroit

<davy@riacs.edu> Thu, 25 May 89 19:01:31 -0700

Taken from the San Jose Mercury News, 5/25/89 (Knight-Ridder News Service).

DETROIT - Secret Serviceagents smashed what they described as a costly, sophisticated computer intrusion network Wednesday and were surprised to discover it made up largely of teen-agers.

The computer systems of more than 20 companies including the Michigan Department of Treasury and Home Box Office cable television services, were infiltrated, according to agents serving search warrants across the country.

Federal officials said the infiltrations by the network represented fraud of \$200,000 to \$1.5 million in appropriated goods, telephone and computer time.

Agents expected to arrest some adults when they swept down on eight people who allegedly ran the network in several states. Instead, they found only one adult, in Chicago. The rest were teen-agers as young as 14: two in Columbus, Ohio; two in Boston; two in Sterling Heights, Mich.; and one in Atlanta. Agents expected to make another arrest in Los Angeles.

Officials said at least 55 other people nationwide made use of the network's information.

In Sterling Heights, Secret Service agents pulled two eighth-grader boys, both 14, out of school and questioned them in the presence of their parents, who apparently were unaware of their activities. James Huse, special agent in charge of the U.S. Secret Service office in Detroit, said the youths admitted involvement in the scheme.

He said the eight-graders [sic], because they are juveniles, cannot be charged under federal law and will be dealt with by local juvenile authorities.

Authorities believe the mastermind is Lynn Doucett, 35, of Chicago. She was arrested Wednesday and is cooperating with authorities, Huse said.

Doucett, who was convicted in Canada of telecommunications fraud, supports herself and two children through her computer intrusion activities, which include using stolen or couterfeit credit cards for cash advances or money orders, according to an affidavit filed in U.S. District Court.

If convicted, she faces up to 10 years in prison and a \$250,000 fine.

# Robert T. Morris suspended from Cornell

<davy@riacs.edu> Thu, 25 May 89 18:49:38 -0700

Taken from San Jose Mercury News, 5/25/89 (From the New York Times)

Cornell University has suspended the graduate student identified by school officials as the author of [the Internet worm].

In a May 16 letter to Robert Tappan Moris, 23, the dean of the Cornell University Graduate School said a university panel had found him guilty of violating the school's Code of Academic Integrity.

He will be suspended until the beginning of the fall semester of 1990, and then could reapply.

No criminal charges have been filed against Morris. A federal grand jury this year forwarded its recommendations to the Justice Department, which has not taken any action. [....]



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 8: Issue 75

Tuesday 30 May 1989

# Contents

- Mariner I -- no holds BARred **PGN**
- Another false incarceration **PGN**
- Perfecting Peopleware **Bob Morris**
- Aegis and the Iranian Airbus shootdown Steve Philipson
- Radio Frequency interference

J. Michael Berkley

SRI attacked by kamikaze squirrels?

David L. Edwards

- Computer electrocutes chess player who beat it! **Gene Spafford**
- Info on RISKS (comp.risks)

#### Mariner I -- no holds BARred

Peter Neumann < neumann@csl.sri.com> Sat, 27 May 1989 15:34:33 PDT

Paul Ceruzzi has written a truly outstanding book for the new show that opened two weeks ago at the Smithsonian National Air and Space Museum. The exhibit and the book are both entitled "Beyond the Limits -- Flight Enters the Computer Age". Both are superb. Go for it (them).

Paul has dug into several cases treated previously in RISKS and in issues of the ACM Software Engineering Notes, and has been able to resolve several mysteries. In particular he considers the case of Mariner I, about which various inaccurate stories have been told. Intended to be the first US spacecraft to visit another planet, it was destroyed by a range officer on 22 July 1962 when it behaved erratically four minutes after launch. The alleged missing 'hyphen' was really a missing 'bar'. I quote from Paul's book, pp. 202-203:

During the launch the Atlas booster rocket was guided with the help of two radar systems. One, the Rate System, measured the velocity of the rocket as it ascended through the atmosphere. The other, the Track Ssytem, measured its distance and angle from a tracking antenna near the launch site. At the Cape a guidance computer processed these signals and sent control signals back to the tracking system, which in turn sent signals to the rocket. Its primary function was to ensure a proper separation from the Atlas booster and ignition of the Agena upper stage, which was to carry the Mariner Spacecraft to Venus.

Timing for the two radar systems was separated by a difference of forty-three milliseconds. To compensate, the computer was instructed to add fourty-three milliseconds to the data from the Rate System during the launch. This action, which set both systems to the same sampling time base, required smoothed, or averaged, track data, obtained by an earlier computation, not the raw velocity data relayed directly from the track radar. The symbol for this smoothed data was ... `R dot bar n' [R overstruck `.' and `\_' and subscript n], where R stands for the radius, the dot for the first derivative (i.e., the velocity), the bar for smoothed data, and n for the increment.

The bar was left out of the hand-written guidance equations. [A footnote cites interviews with John Norton and General Jack Albert.] Then during launch the on-board Rate System hardware failed. That in itself should not have jeopardized the mission, as the Track System radar was working and could have handled the ascent. But because of the missing bar in the guidance equations, the computer was processing the track data incorrectly. [Paul's EndNote amplifies: The Mariner I failure was thus a {\it combination} of a hardware failure and the software bug. The same flawed program had been used in several earlier Ranger launches with no ill effects.] The result was erroneous information that velocity was fluctuating in an erratic and unpredictable manner, for which the computer tried to compensate by sending correction signals back to the rocket. In fact the rocket was ascending smoothly and needed no such correction. The result was {\it genuine} instead of phantom erratic behavior, which led the range safety officer to destroy the missile, and with it the Mariner spacecraft. Mariner I, its systems functioning normally, plunged into the Atlantic.

#### Another false incarceration

Peter Neumann <neumann@csl.sri.com> Sat, 27 May 1989 16:22:24 PDT

In his testimony on 18 May 1989 to the Subcommittee on Civil and Constitutional Rights of the Committee on the Judiciary of the U.S. House of Representatives, relating to the National Crime Information Center (see Bob Morris, RISKS-8.27), David D. Redell (redell@src.dec.com) cited another case of false incarceration (see the case of Roberto Perales Hernandez, noted by Rodney Hoffman in RISKS-8.71, as well as various cases noted earlier -- such as that of Terry Dean Rogan):

"Only last week, a case in California demonstrated the potential benefit of

easy access to stored images. Joseph O. Robertson had been arrested, extradited, charged, and sent to a state mental facility for 17 months. During that entire time, mug shots and fingerprints were already on file showing clearly that he was the wrong man, but no one had taken the trouble to check them."

### Perfecting Peopleware [Governing Magazine]

<RMorris@DOCKMASTER.NCSC.MIL>
Wed, 24 May 89 17:04 EDT

Perfecting Peopleware by Rob Gurwitt

[extracted from Governing Magazine, May, 1989.]

A few years back, Liz Krueger noticed a pattern to the calls she was receiving from New York City's network of activists for the poor. They were phoning her to report that their clients, in rising numbers, were having trouble getting their welfare checks and food stamps on time. Far from being scattered at random throughout the city's five boroughs, it turned out, the troubles clustered around particular "income maintenance centers," city offices that handle public assistance payments.

All the centers involved, Krueger discovered, had been tied in to the new Welfare Management System, a massive computerized network through which, at state orders, the city was to manage public assistance, food stamps and Medicaid disbursements. "I could see very clearly that you started to have crises in centers approximately six weeks after they started to go into conversion," says Krueger, associate director of the Community Food Resource Center, a Manhattan advocacy group. New York's social welfare delivery efforts, in short, were being derailed by computer problems.

This was not a case of hardware gone on the fritz or of software paralyzed by bugs, however. It was a problem with the human part of the system.

In the years before the state imposed the new Welfare Management System on them, city welfare officials had used their own computerized system to keep track of recipients and payments. But the new system worked differently, and social service workers were suddenly faced with hundreds of new codes to learn - codes describing school-age children, or young mothers who had dropped out of school, or able-bodied men looking for work. At their terminals in hectic offices, under pressure to keep up with their immense caseloads, city workers were, not surprisingly, making mistakes.

When someone trying to describe, say, a 35-year-old mother of five instead entered the code for a 20-year-old male high school dropout, the system would check the profile against existing city and state records, and find that the worker's entry contradicted information about the recipient in those other data bases. Until the discrepancy could be cleared up, which might take weeks, no payment would go out.

Advocates for the pool say that welfare centers recorded error rates as high as 30 or 40 percent; the city says that the rate only went as high as 20 percent. Whatever the case, thousands of New York City's poorest residents were suddenly cut off from desperately needed income. "When the rent's due", says Krueger, "landlords are not interested in hearing stories about the city and the state having computer problems, and supermarkets are not interested in the notion of credit."

For all concerned, it was a bruising and expensive lesson in technological change. What the city was discovering - as other jurisdictions had before it, and yet others are still doomed to do - was that in making a computer system work, technical success is meaningless on its own. Unless handled with care and forethought, knotty human and organizational problems can confound a new system as effectively as any latter-day Luddite.

[The article continues for several pages of well-thought-out and well-written commentary on people/computer interfaces and the organizational issues of introducing a new computer system.]

# Aegis and the Iranian Airbus shootdown (RISKS-8.74)

Steve Philipson <steve@aurora.arc.nasa.gov> Fri, 26 May 89 20:08:32 PDT

In <u>RISKS-8.74</u>, Peter Neumann summarized comments made by Matt Jaffe on the design of the Aegis system, in the context of the Vincennes / Iranian Airbus incident. I had the opportunity to read a copy of the de-classified report on this incident and feel obliged to make a few clarifications. Unfortunately, I do not have a copy of the report, so I can't quote from it, thus these observations are from memory.

An initial IFF interrogation showed a Mode II return AND a discreet ID code that had been in use by aircraft confirmed to be Iranian F-14s in earlier operations. One explanation was:

[...] What may have happened was that the airliner taxied near enough to an F-14 on the ground as to preclude the system from recognizing that there were in fact TWO aircraft.

The computer records showed that the radar "range gate", i.e. the area which it was listening to, had been set on the airport for an extended period of time. It was considered quite likely that due to atmospheric ducting effects, an F-14 on the ground and powered-up may have responded to a radar interrogation after the Airbus was airborne. This caused association of this single return with the unknown aircraft, and predisposed the crew to believe that it was an F-14.

Once the airliner was airborne, its lack of further mode II activity would not preclude the display of the old Mode II code. Aircraft may fail to respond to an IFF interrogation (of any code) for a variety of reasons and yet operators (both civil and military) want to have the last received code remain displayed.

The above does not agree with the official report. The Vincennes interrogated the unknown aircraft several times, and received Mode III replies with altitude information. The Mode II return was not repeated, and the Mode III replies were clearly displayed. Each new return was shown with the current altitude return.

It seems that a single junior officer misinterpreted his display to indicate that the aircraft was descending and accelerating on an attack profile towards the Vincennes. He made several call-outs to that effect even though his display showed otherwise. It seems likely that he had mentally fixed on the idea that the unknown aircraft was a hostile threat, and was seeing on his display what he believed would be happening rather than what was happening. A more senior officer accepted these statements and relayed the information to the captain. The senior officer was stationed at a console that also displayed the altitude and mode information, but he did not independently verify it.

The captain was receiving inputs from several sources to the effect that the unknown aircraft was descending and accelerating. He chose to fire on that information. Unfortunately, those sources were all basically the same source -- the statements of the junior officer.

The situation in the ship's combat center must be appreciated to understand this incident. The ship was maneuvering radically and in engagement with highly maneuverable small surface boats. Small bore fire from the boats was impacting the hull of the Vincennes, and fire was being returned. The crew perceived a hostile aircraft threat to be closing on their ship. They thought the aircraft was off of assigned airways as their displays of the airway were several miles off from their correct position (I don't recall the reason why), and they did not have information on the schedules of departures from this airport. The intercom lines were very active and some people were shouting. This was an atmosphere of extreme tension and confusion -- just as we might expect in battle. Even so, at least one officer called "possible com-air" (commercial airliner) several times, but his calls did not gain enough credence to prevent the firing of missiles.

The Aegis system is not just a safety-critical system, it is a battle system. As such, it must be evaluated as to how well it reaches its objectives in a battlefield environment. The outcome here was mixed -- the ship was protected, but an innocent was destroyed. It is clear that a battlefield is no place for innocents. It may also be the case that a system like the Aegis cannot be used where there is much civilian traffic mixed-in with fighting craft. Perhaps no system can function in this environment without a chance of such an accident occurring. The battle doctrine may simply be incompatible with civilian traffic. This is nothing new -- WWII pilots made a point of staying away from friendly ships to avoid being shot down. If identity was in doubt, it was preferable to shoot down a friendly aircraft than to lose a ship.

No equipment necessary for the Vincennes mission could have prevented a manual decision from being difficult, nerve-wracking, and error-prone.

This is true, but a system with a less ambiguous display of critical

information could make errors less likely. Better definition of roles and responsibilities in the combat center could also help to minimize error. This is not just a computer system problem, but a human problem. There are problems in trusting technology under adverse circumstances, but there are also problems with trusting human beings. When we build systems, we must take into account both the strengths and weakness of computers AND of people.

#### Radio Frequency interference

"J. Michael Berkley" <jmberkley@watnext.waterloo.edu> Tue, 23 May 89 20:30:14 EDT

An interesting article from the Kitchener-Waterloo Record:

"THUNDER BAY (CP) - An accident that killed a miner in Northern Ontario in March has 'frightening' implications for other mine workers, a coroner said Thursday.

"Gerry Urchel, 37, fell 24 metres to his death after being pushed off a ledge by a piece of radio-controlled machinery, a coroner's inquest heard.

"Two machines had been set accidentally on the same radio frequency, the inquest was told. One machine - a scoop tram - lurched forward after it picked up a radio signal meant for the other machine."

There is more in the article, but this is the part that is relevant to RISKS.

I must admit, I am surprised that there are no safeguards against this sort of thing already. What kind of safeguards are possible in this situation and are the safeguards reliable?

Mike Berkley, University of Waterloo, PAMI Lab

#### SRI attacked by kamikaze squirrels?

David L. Edwards <dle@csl.sri.com> Mon, 29 May 1989 20:06:25 PDT

It seems that SRI's "no-single-point-of-failure" power system failed at the hands, er the paws, of a squirrel. It was an unsuccessful attempt to ensure that we all got today off.

The power was off for approximately 9 hours. CSL was fully operational by 6:30 PM. We experienced no hardware problems as of yet but the next 72 hours will be the test.

The network is operational and most hosts around the institute are running. SRI-NIC is currently down but being repaired. KL is down.

-dle

[This is at least the third time in my SRI experience that a squirrel has done SRI in. Since the previous incident -- which took us down for something like four days -- we have established a cogeneration plant which together with isolation, standby generators, and PG&E were supposed to guarantee us safe power. The paws that refresh would have been nice for a holiday, except that David came in to minimize the damage on restoral, and this was the second Sunday in a row that an all-day power outage had kept me from trying to catch up on-line, in the midst of travelling. PGN]

## Computer electrocutes chess player who beat it!

Gene Spafford <spaf@cs.purdue.edu> Mon, 29 May 89 12:50:22 -0500

14 March 1989 issue of "Weekly World News" [one of those supermarket tabloids]

Computer Charged with Murder After Frying Chess Champ, by Ragan Dunn

A Soviet super-computer has been ordered to stand trial for the murder of chess champion Nikolai Gudkov -- who was electrocuted when he touched the metal board that he and the machine were playing on! "This was no accident -- it was cold-blooded murder," Soviet police investigator Alexei Shainev told reporters in Moscow. "Niko Gudkov won three straight games and the computer couldn't stand it. When the chess master reached for his knight to begin play in the fourth game, the computer sent a lethal surge of electricity to the board surface. The computer had been programmed to move its chess pieces by producing a low-level electric current. "Gudkov was electrocuted while a gallery of hundreds watched."

The decision to put the computer on trial stunned legal experts around the world. [I hope computer experts are also shocked, so to speak. --spaf] But the Soviets are convinced that the computer had the pride and intelligence to develop a hatred for Gudkov -- and the motive and means to kill him. The mind-boggling murder drama unfolded during a six-day chess marathon between the M2-11 supercomputer and Gudkov, a world class chess player.

According to reports, Gudkov defied all odds [Calculated by the same supercomputer, no doubt. --spaf] and beat the machine in three consecutive games. And when they prepared to begin their fourth, a deadly dose of electricity flowed up into the electronic board and zapped Gudkov dead. Soviet authorities initially thought that the surge of electricity was caused by a short-circuit. But an examination of the computer revealed no problems.

It was later determined that the machine diverted the flow of electricity from its brain to the chess board to ensure a victory over Gudkov. [This implies that Soviet semiconductors work at voltages of a few hundred volts, or maybe their supercomputers are tube-based? --spaf]

"The computer was programmed to win at chess and when it couldn't do that legitimately, it killed its opponent," said investigator Shalnev. "It might sound ridiculous to bring a machine to trial for murder. [!!] But a machine that can solve problems and think [sic] faster than any human must be held

accountable for its actions."

Rudi Hagemann, the Swiss legal scholar, agreed with the Soviet cop. He said that the development of artificial intelligence has come so far in recent years that certain computers and some robots "must be considered human."

It isn't clear how the Soviets will punish the computer if it is found guilty when it goes to court this spring. [Send it to a Gulag for reprogramming? --spaf]

But Hagermann says the machine will probably be reprogrammed or dismantled altogether.

[I don't think there's much to say here, except in the way of warning: next time you accuse the system of cheating at rogue, don't say it too loudly! -spaf]

[This reminds me of the WWN story from 10 July 1984 about the 58-year-old Chinese man, Chin Soo Ying, who had designed a computer system in 1950 (based on the British Colossus) to express words of love and emotions. The article related how after he had built a new machine in the 80s, he was electrocuted by the old machine. His wife was convinced that Chin was murdered by the old machine, which then committed suicide. (The WWN hadline was "Jealous Computer Zaps its Creator".) I recall this in the interest of perspective on the current story, and its source. 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 8: Issue 76

# Wednesday 31 May 1989

#### **Contents**

State computer system scrapped

**Davis** 

- Swedish library loan data to become secret **Howard Gayle**
- SABRE

**Bill Murray** 

Strange Customs Service Clock Department

Willis H. Ware

- No power lunch, just no-power crunch (after the squirrel's over)
- Re: Computer electrocutes chess player who beat it! **David Chase**
- Five admit automated teller scam **Rodney Hoffman**
- Re: Kevin Mitnick Kenneth Siani
- Info on RISKS (comp.risks)

## ✓ State computer system scrapped (RISKS-8.73)

<davis@ai.mit.edu>

Tue, 30 May 89 11:02:49 edt

Rumor: Al Causes \$20M Loss to Pennsylvania

How Rumors Get Started, Lesson 1 (Excerpts from Seattle Times article quoted by Bruce Forstall in Risks 8.73):

#### Quote 1:

COSMOS, designed by Pennsylvania-based UNISYS Corp., was thought so advanced that Gov. Booth Gardner and some of the state's computer professionals likened it to ``artificial intelligence."

## Quote 2:

"This was an effort to create artificial intelligence so the computer could 'think' about eligibility," Gardner said yesterday. "I don't think we'll mess with artificial intelligence again."

Notice the shift from ``likened it to Al'' to ``an effort to create Al.''

Notice how what starts out being metaphorical turns literal. Does the system in fact use any Al techniques? Impossible to tell. But what's the lingering impression and what will people likely remember?

## Swedish library loan data to become secret

Howard Gayle <howard@dahlbeck.ericsson.se> Tue, 30 May 89 15:22:36 +0200

This is based on an article in the Stockholm newspaper Dagens Nyheter, 29 May 1989, p. 25. The Swedish parliament has just passed a law, effective 1 October 1989, making the records of public library loans secret. At present, such records are in principle public information, so that any person can find out which books any library patron has borrowed. In practice some libraries refuse to give out such information, although this is technically illegal. The minister of justice opposed the new law, although the article does not say why. Like all Swedish laws, there are plenty of exceptions. Data may be released if the release does no harm, if the patron borrows technical literature for use at work, if the data are needed to calculate compensation to authors, or if the data are to be used for research. (Authors get some money based on how many times their books are borrowed, in addition to royalties.)

#### **✓ SABRE**

<WHMurray@DOCKMASTER.NCSC.MIL>
Sat, 27 May 89 13:55 EDT

>Is SABRE is too tightly coupled to its hardware to be moved to a >platform that provides hardware memory protection? Or is it just plain >too big to be ported?

SABRE, like most reservation systems, runs on ACP or TPF. These high-performance, limited function operating systems run on hardware with memory protection, i.e., 370 XA. However, for performance reasons, they do not exploit the isolation features of the hardware. All application code runs in a single address space and at the same level of privilege.

While this strategy is inherently dangerous, there are compensating controls imposed on application code. The strategy has been very successful. The res systems have achieved extraordinary reliability and stability for any kind of system, let alone systems which are both mammoth and monolithic.

Portability is another issue. Like most application code, the code of the res systems is sensitive to its environment. It expects a certain application program interface. It can run anywhere it sees that API. The API isolates it from the underlying hardware and operating system. The application code has survived many ports to new hardware and operating system.

However, the application is so large and complex that it is difficult to view it as anything but a monolith. The monolith can only be ported as a whole to something big enough to contain it. IBM is under continual pressure to expand the environment fast enough to accommodate the growth of the application, and the operators struggle to keep it small enough to run in the biggest system available.

If you were to begin today, knowing what we know, you would never permit anything so large and monolithic to come into existence. On the other hand it is too large, important, valuable, and vital to kill. Like many other successful applications from the sixties, it has a life of its own. While we may migrate many of its functions to compartmented sub-systems, the core is likely to be with us for a very long time.

Success is like that.

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

## Strange Customs Service Clock Department

"Willis H. Ware" <willis@rand.org> Fri, 26 May 89 17:13:34 PDT

[Excerpted and Paraphrased from Government Computer News, May 1, 1989, pg 6, byline of Vanessa Jo Grimm.]

The U.S. attorney for Washington is reviewing an allegation that a Customs Service official violated the Computer Security Act [PL 100-235 presumably] by altering a computer's internal clock.

Treasury Department Inspector General Michael R. Hill referred the allegation to the prosecutor after an investigation into year-end spedning by Custom officials at the close of FY 1988. The allegation involves an official who may have authorized altering the date maintained by the computers [that] the agency uses for procurment documents, according to Maurice S. Moody, the IG's audit director for Financial Management Service.

Moody recently told the House Ways and Means Subcommittee on Oversight the computers are part of the agency's Automated Commercial System. He declined to provide GCN with more details.

Allegedly the computer clock was rolled back during the first three days of October [of 1988] so that \$41.8M in procurement obligations would be dated in September against FY 1988 appropriations, Moody said.

An IG report issued in late February concluded Customs had not violated

any procurement laws. The IG's investigation is continuing, however.

"Doesn't \$41.8M worth of procurement on the last day of the fiscal year bother anybody?" asked Rep. Richard T. Shulze (R-Pa). The purchases did bother the IG, Moody said, and this concern led to getting the US attorney. "This problem is endemic in the federal government," he said. "Year-end spedning is very common."

William F. Riley, Customs controller, said he knew about the rollback, but he and Deputy Commissioner Michael H. Lane refused to say who authorized the action... Subcommittee members continued to press Riley and Lane. "Is the person still at Customs?" asked subcommittee chairman J.J.Pickle (D-Texas). "He is working full time and in the position he was at the time," Lane answered.

Rep. Beryl F. Anthony, Jr. (D-Ark) asked how Riley became aware of the rollback. "He [the official who authorized the rollback] told me that it was going to be done," Riley said.

[Rep Pickle suggested that a high ranking official would have to authorize such an action, but Counsel advised Lane not to reply. He did say neither he nor Commissioner von Raab had made the decision.]

[The balance of the article deals with the actions of Linda Gibbs, who became aware of the incident and reported it to the IG after being unable to stop the action. Gibbs also alleged that the action was intended to use available year-end money to cover cost overrun on a contract with Northrop Corp. She also alleged that she had been reassigned and given no new duties.]

#### ✓ No power lunch, just no-power crunch

Peter Neumann <neumann@csl.sri.com> Wed, 31 May 1989 14:30:35 PDT

When people returned to work on Tuesday after Monday's squirrel attack (noted in RISKS-8.75), at least NINE Sun monitors had been wiped out at SRI. Sun was terrific in having replacements for most by Tuesday afternoon. (The DEC mainframes that Dave Edwards noted had been downed both took a while to bring up again -- including our friendly old DEC 2065 KL, which I shall miss when it finally gets decommissioned.)

## ★ Re: Computer electrocutes chess player who beat it! (RISKS 8.75)

<chase@orc.olivetti.com>
Tue, 30 May 89 13:18:07 -0700

- > This implies that Soviet semiconductors work at voltages of a few
- > hundred volts, or maybe their supercomputers are tube-based?

The story as it stands sounds bogus, but don't discount low voltages. One of the worst shocks I've ever received (in the range of 6 to 12000 non-static volts) was only 12 volts. I was VERY well grounded (driving in the rain in a car with old metal springs in the seats and big holes in the floor), and attempted to manipulate the metal stump of the wiper control with a finger with a cut on the end of it. The sensation was something like a whack across the chest with a baseball bat. Normally, I can't even feel 12 volts.

David

[Maybe the WWN writer got it wrong, and it was "chest" instead of "chess"?

#### Five admit automated teller scam

Rodney Hoffman < Hoffman. El Segundo @ Xerox.com > 24 May 89 08:33:57 PDT (Wednesday)

In RISKS-8.24, I summarized a news account about five people arrested and charged with violating federal fraud statutes in a scheme to use more than 7,000 counterfeit ATM cards. The alleged mastermind, Mark Koenig, was a computer programmer who, while temporarily working under contract on a job dealing with several hundred ATMs, transferred bank account and PIN information to his home computer and stole an ATM encoding machine from his office. He and his confederates planned to use the counterfeit ATM cards to withdraw cash from ATMS throughout California and the Midwest over the three-day Presidents Day weekend in February. An unnamed informant alerted the U.S. Secret Service, who arrested the five people before that holiday weekend.

A wire service story in the LATimes 23-May-89 reports that the five pleaded guilty Monday. All are scheduled for sentencing Aug. 25, and face prison terms of up to 72 years each.

## ★ Re: Kevin Mitnick < Armed with a Keyboard and Considered Dangerous >

<SIANI@nssdca.GSFC.NASA.GOV> Tue, 23 May 89 09:53:47 EST

Kevin Mitnick, the hacker "so dangerous that he can't even be allowed to use a phone". "He could ruin your life with his keyboard". "Armed with a keyboard and considered dangerous."

These are some of the things that have been said about this person. All of this media hype would be fine if it just sold news papers. But it has done much more then just sell a few papers. It has influenced those that will ultimately decide his fate. I myself don't know the man, but I have talked to others that do. Including one of the persons that investigated Mitnick. From all I have heard about him, I think he is a slime ball! But even a slime ball should not be railroaded into a prison sentence that others of equal or greater guilt have avoided.

I personally feel the man is just a criminal, like the guy that robs a 7/11, no better but certainly not any worse. Unfortunately he is thought of as some kind of a "SUPER HACKER". The head of LA Police Dept's Computer Crime Unit is quoted as saying "Mitnick is several levels above what you would characterize as a computer hacker".

No disrespect intended, but a statement like this from the head of a computer crime unit indicates his ignorance on the ability of hackers and phone phreaks. Sure he did things like access and perhaps even altered Police Dept. criminal records, credit records at TRW Corp, and Pacific Telephone, disconnecting phones of people he didn't like etc. But what is not understood by most people outside of the hack/phreak world is that these things are VERY EASY TO DO AND ARE DONE ALL THE TIME. In the hack/phreak community such manipulation of computer and phone systems is all to easy. I see nothing special about his ability to do this. The only thing special about Kevin Mitnick is that he is not a "novice" hacker like most of the thirteen year old kids that get busted for hacking/phreaking. It has been a number of years since an "advanced" hacker has been arrested. Not since the days of the Inner Circle gang have law enforcement authorities had to deal with a hacker working at this level of ability. As a general rule, advanced hackers do not get caught because of there activity but rather it is almost always others that turn them in. It is therefore easy to understand why his abilities are perceived as being extraordinary when in fact they are not.

Because of all the media hype this case has received I'm afraid that:

- 1.) He will not be treated fairly. He will be judged as a much greater threat to society then others that have committed simular crimes.
- 2.) He will become some kind of folk hero. A Jesse James with a keyboard. This will only cause other to follow in his footsteps.

I'm not defending him or the things he has done in any sense. All I'm saying is let's be fair. Judge the man by the facts, not the headlines.

Disclaimer: The views expressed here are my own.

Kenneth Siani, Sr. Security Specialist, Information Systems Div., NYMA Inc.



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 8: Issue 77

Thursday 8 June 1989

## Contents

Second elevator death

**Walter Roberson** 

Electronic card spots hooligans

**Martyn Thomas** 

Big Brother is watching your magnetic card

**Amos Shapir** 

May you live in interesting times (High-tech Chinese revolution)

**Martin Minow** 

"Core-Walker" that crashed SABRE

**Rodney Hoffman** 

Airbus A320

**Brian Randell** 

Re: Power outages

Peter Scott

One of Cliff Stoll's `Wily Hacker' dead (suicide?)

Klaus Brunnstein

Computer Virus Catalogue (Aims and Scope)

Klaus Brunnstein

Info on RISKS (comp.risks)

#### Second elevator death

<Walter Roberson@CARLETON.CA> Mon, 05 Jun 89 17:48:03 EST

Early last week, we had a second elevator fatality in Ottawa. In this case, the person was caught by the doors closing as they were stepping in. The elevator went up and down several floors before they were able to stop it and get the fellow out. The problem was apparently an electrical problem with the door interlock circuits that allowed the elevator to move with only one of the doors closed. The elevator (made by Otis in about 1954) had been serviced earlier that same day. Those of you that remember the incident earlier this year in Ottawa, wherein a 13 year old girl was killed, might recall that -thatelevator had been serviced earlier the same day. The local paper never did,

though, publish the results of the inquest into that death, so I still don't know what the problem was in that case. People have been rumbling louder about the politics in that case (the building was largely populated by people waiting for their immigration applications to be heard) than about the mechanics of the elevator.

Walter Roberson < Walter Roberson@Carleton.CA>

#### Electronic card spots hooligans

Martyn Thomas <mct@praxis.UUCP> Tue, 6 Jun 89 10:45:16 BST

The following article appeared in the June 1st issue of Electronics Times, a respected trade newspaper of the UK electonics industry. It raises many questions, ranging from technical feasibility to security, privacy, and admissability of evidence. Have RISKS readers any information on this technology?

#### **ELECTRONIC CARD SPOTS HOOLIGANS**

Football hooligans could find their activities curbed by electronics, thanks to a new surveillance system developed in Italy. The Hooligan Stopper can pick out individual trouble makers and warn of impending violence.

Manufacturers AGM Electronica and MEG Italia designed the system with UK football fans in mind. They claim it can cope with crowds of up to 130 000 and could replace 10 000 police officers.

Supporters gain access to the stadium with an electronic personal card (epc), while transponders sense the occurrence of disturbances and relay information back to a central tranceiver and data processing system.

Franco Bertuzzi, the system's inventor, declined to identify the West german electronics company that is manufacturing the device and refused to give details of the ics and sensors used.

"All I can say is that the microchip in the epc starts to function when the card owner becomes violent, lashing out at other spectators or running amok", he said.

Bertuzzi said the card did not even have to be in direct contact with the owner to pick up 'agitation signals'. "It is already used in high level security systems in the civilian and military sectors," he said.

"By reading the data the interceptors pick up from the magnetic strip, all the personal details of the card's owner can be known immediately."

The epc could be sold for #20 [UK pounds] and be used to gain admission to several matches. By charging for the card, fans would be discouraged from throwing it away, which they might be tempted to do if it exposed them to detection if they became violent or unruly.

Installation costs for a stadium the size of Wembley would be around #1.5 million [UK pounds].

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK. Tel: +44-225-444700. Email: ...!uunet!mcvax!ukc!praxis!mct

["WEMBLEY? I thought this was TUESDAY."

"Oh, you're right. How do we get the cards TO STAY in people's pockets?" <I imagine spectators setting up a check-your-card service with their favorite designated nondrinker, who might even charge a fee.> PGN]

## Big Brother is watching your magnetic card

Amos Shapir <amos@taux01.UUCP> 1 Jun 89 14:37:41 GMT

Remember all those articles in RISKS about governments and institutions being able to track people using data about their magnetic ATM or credit cards? Well, the nightmare has come true: a system specifically designed to track people will be in use shortly. The military government of Israel's occupied territories announced that all residents wishing to work in Israel will be given magnetic-striped work permit cards. An electronic turnstyle will keep track of their movements across the border at all entry points.

Amos Shapir, National Semiconductor (Israel) P.O.B. 3007, Herzlia 46104, Israel Tel. +972 52 522261 TWX: 33691, fax: +972-52-558322

## ✓ May you live in interesting times (High-tech Chinese revolution)

Repent! Godot is coming soon! Repent! <minow%thundr.DEC@decwrl.dec.com> 5 Jun 89 11:23

I wonder whether DARPA (and other governmental sources of funding) ever thought that "the network" would be used to organize a revolution?

To see the process unfolding, you might consider reading through the Usenet soc.culture.china, which currently has a combination of news, rumor, fax and telephone numbers for university student unions in China, polemics, speculation, and the telephone/internet address of student committees all over the world.

Martin Minow

## "Core-Walker" that crashed SABRE

Rodney Hoffman <Hoffman.ElSegundo@Xerox.com> 5 Jun 89 14:32:06 PDT (Monday)

THE 'CORE WALKER' THAT STALLED AMERICAN AIRLINES

('Business Week' 12-June-89, page 98C)

The computer foul-up that shut down American Airlines Inc.'s Sabre ticketing system for 12 hours after midnight on May 12 [see related notes <u>RISKS 8.71</u>, 8.74, and 8.76] was not caused by human error or sabotage, the company's investigators have found. Instead, it was apparently the result of a glitch that was written into the system but never showed up until now. "We call it a core-walker," says an American spokesperson, "because it literally walked through the system."

The problem began when American tried to add a pair of mammoth disk drives to the nation's largest computerized reservations system. Suddenly, the program accompanying the new disk drives changed a piece of information in the software directing the activities of the 1,080 existing Sabre disk drives. Once embedded, this new bit of data jumped from one disk drive to another and stripped away the names of files stored on them, making it impossible for American's computers to retrieve the information on the drives. To solve the problem, American is revamping its disk-drive software. According to the airline, revenue losses during the Sabre shutdown were minimal.

#### Airbus A320 (Updating earlier report in RISKS-8.57)

Brian Randell <Brian.Randell@newcastle.ac.uk> Fri, 2 Jun 89 18:27:25 BST

The Observer, which is a well-respected UK Sunday newspaper, on 28 May 1989 carried a lengthy article about the A320. It contains more explicit allegations about computer-related problems than I had seen before, so below I quote relevant sections. [Brian Randell, Computing Laboratory, University of Newcastle upon Tyne]

AIRBUS CRASH: WAS THE PILOT THE FALL GUY

Open File: Jim Beatson finds that the evidence points to computer failure.

"On June 26, 1988, Air France's new European A320 Airbus, delivered only two days previously, crashed into trees at an airshow near Mulhouse in France while performing a low-level pass. Three passengers - a woman and two children - were killed. The pilot, Michel Asseline, a senior Air France captain and the man inaugurating the new model, as well as being its chief instructor, escaped unhurt.

After the accident, the European aircraft industry waited intently for a verdict on whether the Airbus' new and controversial computerised control system was to blame. The day after the crash Louis Mermar, the French Transport Minister, exonerated the aircraft. Asseline was stood down, accused of flying dangerously, dismissed and stripped of his pilot's licence. But the crash is far from being an open-and-shut case of pilot error.

[Several paragraphs about the flight recorder, and the fact that four seconds of recording, from just before the crash, were lost because the tape was (it is claimed unnecessarily) cut to remove it from the box.]

Captain Asseline is also at odds with Airbus over alleged defects in the aircraft. The pilot claims he was misled on the aircraft's true height by a bug in the software. Normally an aircraft's height is calculated after entering the local barometric pressure into its altimeter. Local ground control provides this to aircraft regularly so that, with each change in barometric pressure, the correct altitude can be displayed. The A320 has a history of occasionally selecting a barometric reading from memory, rather than a current reading, when switching from one flying mode to another. Both British Airways and Air France have experienced this problem with their A320s.

[Paragraphs describing Asseline's claims that he was misled into thinking he was flying at 100 feet, when it was actually 50 to 60 feet, though he admits that there were back-up aural warnings that he failed to heed.]

Finally the pilot claims that the aircraft failed to respond to its throttle. 'I began to push forward the throttle to stabilise my speed reduction', he told Open File. 'At that point I gave the order to disconnect the (automatic) throttle and I'm sure that this movement put a mess in the computer. I push forward the throttles . . . and I had no answer. So I pulled back throttles to zero because I did that many times in training. I knew that if we had any problems with the power, the only thing to do was to close the throttle and then to give full power. That's exactly what I did.'

[Paragraph confirming that, a month before the crash, Airbus put out such instructions.] [Paragraphs about `a young Air France Boeing 747 Pilot, Norbert Jacquet who shared Asseline's belief that the computer fly-by-wire system was partly to blame' and who after going public on this was suspended on `psychological grounds' - disbelieved by fellow pilots - and has since been fired by Air France.]

Two facts are now established about the accident. First, Asseline was asked to fly at 100 feet above the ground - 70 feet less than the normally authorised level. Second, the operational direction and plan supplied by Air France for the display was based on a longer adjoining airstrip than the one Asseline was asked to fly over. On the originally chosen strip, there would have been ample time for the aircraft to throttle up safely over the trees.

Since the crash, other Airbus A320 pilots have also had trouble with their computer controls. One spoke of near disaster flying into Berlin: another of his altimeter 'going crazy' on a descent into Geneva.

British Airways' inaugurating chief pilot, George Hallett, says BA has experienced similar problems. So, was Captain Asseline misled over the aircraft's height, or are they merely claims which he has advanced after the crash to take advantage of known software problems?

Even the aircraft's critics acknowledge that most of its software bugs have now been ironed out. But Captain Xavier Barrell, technical vice-president of Air France's pilots union, SNPL, says the vertical navigation system is still not working properly.

Captain Asseline is now in Los Angeles, trying to gain an American pilot's licence on a Boeing 737 200 series, the same aircraft type on which he did the acceptance launch flights for Air France. The final report of the accident

enquiry is keenly awaited, not just by him and Norbert Jacquet, but also many others."

#### Re: Power outages

Peter Scott <PJS@grouch.JPL.NASA.GOV> Thu, 1 Jun 89 10:24:59 PST

And, on the subject of power outages (RISKS 8.75), \_Science News\_ reports that on May 11 a raccoon electrocuted itself at the University of Utah, causing a 20-second power outage that resulted in a loss of data on the computers being used by Fleischmann & Pons to verify their cold fusion experiments.

'coons have managed to cripple JPL more than once in the past (the last one survived, became a local hero). Obviously small furry animals pose a major threat to installations with single-point-of-failure power systems.

Peter Scott (pjs@grouch.jpl.nasa.gov)

## ✓ One of Cliff Stoll's `Wily Hackers' dead (suicide?)

Klaus Brunnstein <br/> stein%rz.informatik.uni-hamburg.dbp.de@RELAY.CS.NET> 05 Jun 89 10:42 GMT+0100

According to German publications, the 'Wily Hacker' Karl Koch, of Hannover, FR Germany, died Friday last week, probably by suicide. His body was found burnt (with gasoline) to death, in a forest near Celle (a German town near Hannover where he committed his hacks, as had been observed by German Post). Koch was one of the 2 hackers who confessed their role in the KGB hack to the public prosecutors, therewith bringing the case to public attention.

As German newspapers report, he probably suffered from a psychic disease: he thought he was permanently observed by alien beings named Illimunates' which tried to kill him. Probably, he had internalized the role of 'Captain Hagbard' (his pseudonym in the hacking scene), taken from a US book, who (like him) suffered from supervision by the Illuminates. Police officials evidently think that Koch committed suicide (though I learned, that there are 'some circumstances' which may also support other theories; no precise information about such moments are reported).

According to German police experts, K. Koch's role in the KGB case as in daily life can properly be understood when reading this book (which I couldnot get until now, so I cannot control the adequacy of this theory!). Does anybody have more evidence about cases of 'hacking' connected to moments of psychic anomalies, where hackers internalize roles of artificial persons and live in worlds which they internalize after having read corresponding stories?

Klaus Brunnstein University of Hamburg

## Computer Virus Catalogue (Aims and Scope)

Klaus Brunnstein <br/>
<br/>brunnstein%rz.informatik.uni-hamburq.dbp.de@RELAY.CS.NET> 02 Jun 89 14:37 GMT+0100

After having reverse-engineered several viruses on different PCs (AMIGA, Atari, MacIntosh and IBM), we have developped (and experimentally tested, in a German mailbox of the national Informatics society, since December 1988) a format in which we describe essential features of computer viruses: the Computer Virus Catalog. Thanks to Y.Radai, David Ferbrache and Otto Stolz, this Catalog is now available in a revised form. The goal is to describe all those features which a (not too well-informed) user needs to analyse whether and what virus may have reached his machine; moreover, the catalog should contain some hints which established tools help him to erase the virus.

At this time, about 25 viruses (maybe some of which exist in German locations have been catalogued. At the Virus Test Center of Hamburg University/Informatics (with a group of students, who participate in my 4-semester course on Computer Security), we have concentrated on AMIGA and IBM PC viruses, but in the latter case, we have difficulties to get virus code 1) because the German IBM PC virus scene doesnot offer the internationally reported manifold, and 2) we refuse to exchange viruses, like stamps (we also don't publish virus code or the 'dossiers' which we produced by reverse-engineering). We therefore appreciate any help which we can get from competent and cooperative experts in the field.

[The following are in separate documents:

1st: the format of the Computer Virus Catalog,

2nd: the index on entries at this time.]

To minimize the transfer problems to 'remote locations' (seen from a Germanocentric world view), we try to find locations where the actual entries may be invoked (e.g. in US). Moreover, in order to guarantee some degree of completeness, we ask groups/persons with developped knowledge in the field, to take on the task of adding information about viruses not yet catalogued. We plan to establish a committee which controls new or updated entries; while Y.Radai, and D.Ferbrache have accepted to cooperate in this Virus Catalog Editorial Committee, we hope for a few more experts to cooperate in this task.

Thank you in advance for comments. Klaus Brunnstein.

Prof.Dr. Klaus Brunnstein, Faculty for Informatics, Univ. Hamburg,

Schlueterstr.70, D 2000 Hamburg 13, Tel: (40) 4123-4158 / -4162 Secr.

ElMailAdr: Brunnstein@RZ.Informatik.Uni-Hamburg.dbp.de

FromINTERNET:Brunnstein%RZ.Informatik.Uni-Hamburg.dbp.de@Relay.CS.Net FromBITNET: Brunnstein%RZ.Informatik.Uni-Hamburg.dbp.de@DFNGate.Bitnet

FromUUCP: brunnstein%rz.informatik.uni-hamburg.dbp.de@unido.uucp



Report problems with the web pages to the maintainer

The Risks Digest Volume 8: Issue 77		



## 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 8: Issue 78

Sunday 11 June 1989

## Contents

NY Telephone Freebies

**PGN** 

Nielsen Raidings -- A risk?

John Rushby

C-17 Overrun

**Gary Chapman** 

COMPASS '89 reminder

Al Friend

Re: Big Brother is watching your posting in RISKS

**Amos Shapir** 

How Rumors Mutate, Lesson 2

Rich Fritzson

The computer didn't commit the crime

Michael Doob

An ATM gets it right

**Steve Anthony** 

Justice Department wary in Computer Case

Dave Bozak

Info on RISKS (comp.risks)

#### NY Telephone Freebies

Peter Neumann < neumann@csl.sri.com> Sat, 10 Jun 1989 15:53:55 PDT

24 pay phones along the Long Island Expressway were in fact free phones because of a programming/database screw-up. They were being heavily used for long distance calls by those who had discovered the oversight, including many to Pakistan. (Police found 15 Pakistani men using the phones when they went to investigate after a shooting.) There were no estimates on the unrecovered cost of the phone calls. [10 June 1989, San Francisco Chronicle, p. 2.]

#### Nielsen Raidings -- A risk?

John Rushby <RUSHBY@csl.sri.com> Tue 2 May 89 22:11:44-PDT

NEW NIELSEN SYSTEM WILL WATCH THE WATCHERS WATCHING By BILL CARTER c.1989 N.Y. Times News Service, 2 May 1989

NEW YORK -- Soon, some people may be watching television sets that will be watching them back. Nielsen Media Research disclosed plans Wednesday to develop a ``passive people meter'' in conjunction with the David Sarnoff Research Center at Princeton. The device would measure television viewing without relying on the participation of viewers -- a marked departure from Nielsen's current ``people meter'' system, which requires viewers to

Since it began measuring television audiences in 1950, Nielsen has been able to tell when sets in a sample household are on and what channels they are tuned to. The problem has been determining who in the family is watching at any given time. Two years ago Nielsen introduced the people meter to provide that information.

identify themselves by pushing buttons whenever they watch television.

The crucial component of the new system is an image-recognition device that would identify members of a household and record, second by second, when they are watching television, when they leave the room and even when they avert their eyes to read a newspaper.

Nielsen and Sarnoff demonstrated a working model of the device at a news conference Wednesday, at which the issue of invasion of privacy was raised.

Nielsen executives faced questions about the system's similarities to the surveillance of Big Brother in George Orwell's novel ``1984." But Nielsen executives argued that the system will not be intrusive. ``I don't think we're talking about Big Brother here at all," said John A. Dimling, executive vice president of Nielsen Media Research. ``We're not scanning the room to find out what people are doing. We're sensitive to the issue of privacy." Dimling said it will be at least three years before the system goes into service.

The system will consist of a camera-like device and a computer attached to the top of each set in the households in Nielsen's sample group of television viewers. The computer will be programmed to store the facial images of each family member. The camera will be activated each time the set is turned on and will scan the room for faces it recognizes.

The same image-recognition technique has other possible applications, say in medicine and policework. Using a more sophisticated image-recognition system, police could, in theory, scan an airport for known terrorists or drug dealers.

If tested successfully, the passive system would replace the current people meter, which is only two years old. It was meant to provide more precise information about which members of the household were watching particular programs.

The people meters replaced a system, used for 37 years, that relied on viewers filling out diaries. The three major television networks have complained that people meters underestimate actual viewership.

Research executives at the television networks have said that the button-pushing task becomes boring quickly, leading to inaccuracies; that many households refuse to cooperate, and that children cannot reasonably be

expected to push the buttons to indicate when they are watching.

Nielsen now has 4,000 homes in its people-meter survey. But the networks have complained that the current two-year period each household participates in the survey is too long and leads to fatigue.

The network reaction to the people meter is at least partly derived from the effect the system has had on their business.

Nielsen measurements of the networks' share of the audience declined 9 percent immediately after people meters were installed; a decline in ratings means a decline in advertising revenues. A passive system would address most of these complaints, Dimling said. He called the proposed system the ultimate audience measurement, "primarily because the respondents don't have to do anything."

The response to the Nielsen announcement at the networks and in the advertising community Wednesday was favorable. Bart McHugh, senior vice president of DDB Needham, said, "A passive system is what we've all been screaming about."

Alan Wurtzel, senior vice president of research at ABC, said: "I really believe a passive system would be much better. I would hope they would get this out and in place as quickly as possible."

Nielsen reports to clients will include both the number of viewers and demographic data on the makeup of a show's audience. Eventually, Dimling said, networks could know almost instantly which sections of a show the audience was most responsive to, and which bored them enough to make them leave the room, pick up a magazine or fall asleep. Dimling said that only families that agree to participate will be included in the survey.

Under the current people-meter system families are paid a small fee to begin the metering process and are rewarded occasionally with small gifts. Dimling would not say what the monetary incentive for the passive meter system would be.

Curtis Carlson, the director of information systems at Sarnoff, said, `The only information sent back to the Nielsen computers will be whether people are watching television." He said the device will not actually record any other activity. It focuses only on facial features, he said, and decides first if it is a face it recognizes and then if that face is directed toward the set. Unfamiliar faces or even possibly the family dog will be recorded as ``visitors." The system, based on a technique the Sarnoff researchers have labeled ``smart sensing," relies on visual tracking similar to the operation of the human eye, Carlson said. Images on the periphery are screened out, and the camera centers on only the most compelling features.

The current prototype is about as big as a breadbox, Carlson said, and the next step in the development process will be to miniaturize the entire system. The goal is to have a machine about the size and shape of a videocassette recorder.

Nielsen and Sarnoff will also do an extended study and national testing to ensure that the system can meet Nielsen needs before putting it into use.

Nielsen has plans to use the technology in other ways. For example, Nielsen now conducts a market research project in which consumers are asked to use a scanning device to read the product code on articles they buy. But because the people meter requires so much work, Nielsen never asks the same household to participate in both the scanning and people-meter surveys.

Robert R. Brown, president of information services and technology for Nielsen, said the passive people meter could be combined with the scanning survey so Nielsen could track `market stimuli with buying patterns."

Nielsen clients could in theory learn whether television advertising had a direct influence on viewers' buying decisions.

Nielsen has contracted with Sarnoff Research for exclusive use of the technology in the media and marketing area.

Carlson said a different version of the same technology has been applied in at least one other business. He said it was against company policy to disclose which business, but he did say the federal government has expressed interest in the technology. He conceded that as the technology becomes more sophisticated it could open up more questions of privacy. "Every technology can be abused," he said. But he stressed that his laboratory is more interested in possible medical applications. He said, for instance, that the system could eventually be used to increase the reliability of pap smears by using image recognition to identify abnormal cells and could provide a sophisticated object-recognition aid to the blind. Development of both is far down the road, he said.

## ✓ C-17 [Overrun with No Remorse]

Gary Chapman <chapman@csli.Stanford.EDU> Tue, 6 Jun 89 12:47:39 PDT

The June issue of Defense Electronics reports that the manufacturer of the C-17 transport plane, Douglas Aircraft, estimates that software problems in the avionics system of the plane will require a cost overrun of about \*\$500 million.\* The figure was actually an estimate of a Congressional investigation, then confirmed by Douglas. The software is a package with an estimated 750,000 lines of code, as compared to the 25,000 lines of code in a C-5A.

The C-17 is supposed to replace the Air Force's transport aircraft, the C-5A, the C-131, and the C-141. The program was started in 1982, and there are supposed to be 210 C-17s purchased by 1998 at a cost of \$35.7 billion.

There is no detailed information in the short article on what the avionics software problems entail.

-- Gary

#### COMPASS '89 reminder (COMPUTER ASSURANCE) [See RISKS-8.66]

Al Friend <friend@csr.itd.nrl.navy.mil> Fri, 9 Jun 89 22:29:04 edt

> COMPASS '89 IS COMING One week to go!

- => Learn about software safety, risks, and computer assurance.
- => Meet others who are working in these areas.
- => See <u>RISKS-8.66</u> for advance program.

PLACE: National Institute of Standards and Technology \*
Gaithersburg, MD (suburban Washington, DC)
\* formerly National Bureau of Standards

TIME: June 20 - 22 (tutorials on 23rd, other meetings 19th)

CONTACT: Nettie Quartana or Holly Mays at (703) 486-3500

OR: Come directly to COMPASS '89 at NIST.

Register at the door.

FEE: MEMBER/SPONSOR = \$ 225 NONMEMBER = \$ 275

[Let me know if you would like a copy of RISKS-8.66 and cannot FTP it. PGN]

## ★ Re: Big Brother is watching your posting in RISKS

Amos Shapir <amos@taux01.UUCP> 11 Jun 89 10:46:25 GMT

I have just received an anonymous threat to notify my company of my posting in comp.risks ("Big Brother is watching your magnetic card", <u>RISKS-8.77</u>). Let me clarify two points:

- My article was just a summary of what has been published in the local press, and does not necessarily reflect my opinions of the matter.
- My opinions are my own, and in no way represent a policy and/or stand of National Semiconductor Corporation or National Semiconductor (IC) Ltd.

Amos Shapir amos@nsc.com National Semiconductor (Israel) P.O.B. 3007, Herzlia 46104, Israel

[Another Risks of RISKS item! PGN]

## How Rumors Mutate, Lesson 2

<fritzson@PRC.Unisys.COM>
Fri, 2 Jun 89 08:50:17 -0400

>RISKS-FORUM Digest Wednesday 31 May 1989 Volume 8 : Issue 76

>Subject: State computer system scrapped (RISKS-8.73)

>Rumor: AI Causes \$20M Loss to Pennsylvania

>How Rumors Get Started, Lesson 1 (Excerpts from Seattle Times article quoted b

>Bruce Forstall in Risks 8.73):

The article in question was in the Seattle Times because the state that lost the money was Washington, not Pennsylvania.

-Rich Fritzson

#### The computer didn't commit the crime

Michael Doob <mdoob@ccu.umanitoba.ca>

#### 2 Jun 89 10:40 -0500

The Bank of Montreal has two types of billing for checking accounts: (1) a per check charge, or (2) flat rate for an unlimited number of checks. This month, in a burst of creative billing, both charges were applied to the account. What a chance to call it a computer error. Here is what the bank said in a form letter:

We are using the most immediate method to advise that we are correcting an error in the service fees charged to your last True Chequing Account Statement.

We take great care to ensure all account entries are correct and we sincerely regret the human error which caused both monthly

plan fees and per item fees to be charged to some of our customer's accounts. Your next statement will include the appropriate corrections.

Does this mean that blaming the computer will reflect poorly (in the customers' view) on ATM?

#### An ATM gets it right

Steve Anthony <steveo@Think.COM> Fri, 2 Jun 89 11:49:26 EDT

Had an interesting experience with ATM's in the Boston Area last year. I was going on vacation and the mortgage needed to be paid during the vacation. So I made a transfer, at a human teller, from savings to checking to cover it, wrote the check and left for vacation. Upon returning, I got some cash from the ATM and noticed that the balances were not what I expected; savings was too high and checking was too high also. I went thru my receipts and found that I had erred; I made the transfer from checking to savings rather that the other way around. This meant that my mortgage check was going to or had already bounced. I called the mortage bank (different from the checking/savings bank) and inquired about the mortgage payment. I was told that everything was fine; the payment was made. Mystified, I went to my savings/checking bank and asked what happened. I had made the transfer at a BayBank Merrimack Valley branch office and my account is thru BayBank Harvard Trust. As background, in eastern Mass, there is a banking company, BayBanks, that is really a holding company for a variety of individual BayBank companies, two of which are BB Merrimack Valley and BB Harvard Trust. What I was told was that the erroneous transfer had never been made (from checking to savings). I inquired as to why this was so. The person told me that when a transfer is done thru a human teller for an account that is for a different BB company, the transaction may, or maynot get processed; ie it drops into the bit bucket. In order to make sure that a transfer takes place, she suggested that I use the ATM, since there were no known problems with transactions of this type.

So score one for the ATMs.

#### Justice Department wary in Computer Case

Dave Bozak <dab@oswego.oswego.edu> Fri, 2 Jun 89 09:48:41 EDT

Justice Department Wary in Computer Case: Is Washington fearful of losing a landmark trial? by Matthew Spina, Staff Writer

Some computer experts theorize that the Justice Department, afraid of bungling what could become a landmark computer case, still doesn't know how to treat the Cornell student whose computer worm slithered nationwide in November.

A further concern in Washington: A trial in the case might embarrass the Department of Defense if its scientists are asked to detail how their computers were among the thousands crippled by the worm.

For several months, the decision on how to charge 23-year-old Robert T. Morris, Jr. had been before Mark Richard, a deputy assistant attorney general. Within the last few weeks, Richard made a decision that now is being reviewed by an assistant attorney general, according to a computer professional who has been talking with the Justice Department.

"I thought we would have heard something from Washington by now," said Andrew Baxtoer, the assistant U.S. attorney who in November and December presented the case to a grand jury in Syracuse.

The grand jury's report was sent on the the Justice Department, which refuses to comment publicly on the matter because Morris has not been indicted.

"Within the next two weeks I assume that a decision will be made," said one official.

"If they decide to begin an expensive trial, they have to make sure they win so as not to damage future attempts to prosecute under that law," said Eugene H. Spafford, an assistant professor at Purdue University whose analysis of the worm has helped federal investigators. "If they decide not to prosecute, and the total thing that happens is he gets suspended (from Cornell), I will be outraged."

So far, Cornell has taken the only disciplinary measure against Morris, suspending him for the 1989-90 academic year. But the graduate student left the computer science department early in November, the day after the worm spread out of a computer in Upson Hall.

Morris, a computer science graduate student, has been called the author of a rogue computer program, called a worm, that was spread from a Cornell University computer. The program was designed to reproduce and infect any computer linked to the Internet, a network shared by colleges, research centers and military institutions.

However, experts say an error caused the program to replicate out of control, sending thousands of copies into thousands of computers.

If Morris is to be charged with a felony, prosecutors would then have to show he intended to destroy or extract information.

Proving that would be difficult since the program neither destroyed nor removed information from any computer.

To convict Morris on most lesser charges, prosecutors would have to show he intended to harm computers.

Prosecutors also could use a misdemeanor charge requiring them to prove only that Morris gained access to a federal government computer.

The worm did reach computers at the Army Ballistics Research Laboratory and NASA's Langley Research Center, among others.

Some computer experts wonder, though, if Defense Department officials will be reluctant to testify publicly about how their computers were penetrated - even those computers holding non-classified information. In February, at a computer convention in San Diego, Defense Department computer experts detailed some security improvements made to the network since November, but then refused to release copies of their presentation to people at the seminar.

The FBI - which enforces the Computer Fraud and Abuse Act of 1986 - and some people in the computer industry are pushing for a vigorous prosecution to display a strong case against computer hacking. Others in the industry, including some of Morris' friends from Harvard University and Cornell, urge leniency because he was trying to demonstrate security flaws with computers.



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 8: Issue 79

## Wednesday 14 June 1989

### **Contents**

Single point of failure -- Tokyo Stock Exchange

Jerry Carlin

Costly Horse Race

Rick Zaccone

Commercial Loans in California at a Standstill

**PGN** 

Phone Hacking

**Brinton Cooper** 

Microcomputers in the operating theatre

**Martyn Thomas** 

Inspiration from the past -- Machines Will Take Over

**Curtis Galloway** 

"Illuminatus!"

<u>Pete</u>

Praise and Blame -- Computers and People

**Hugh Miller** 

NORAD Computers: Years Late, Unusably Slow, \$207 Million Over Budget

Karl Lehenbauer

Info on RISKS (comp.risks)

#### ✓ single point of failure -- Tokyo Stock Exchange

Jerry Carlin < jmc@PacBell.COM> 12 Jun 89 20:59:51 GMT

"How Tokyo Earthquake Could Destroy the World Economy" SF Chronicle, Monday, June 12, page C7

The reporter quotes a story in "Manhattan, Inc" where it was disclosed that the main and backup computer for the Tokyo Stock Exchange sit right next to each other and in an area totally destroyed by the 1923 earthquake.

This computer is the SOLE repository of Japan's offical records of stock ownership. Therefore if the computer is destroyed, all records of share ownership could disappear with obvious consequences.

The original article speculated on various afteraffects of the earthquake including the collapse of the Yen, bankrupcy of Western insurance companies, and reversal of balance of payments problem.

Jerry Carlin (415) 823-2441 {bellcore, sun, ames, pyramid}!pacbell!jmc

#### Costly Horse Race

Rick Zaccone <zaccone@sol.bucknell.edu> Wed, 14 Jun 89 08:55:25 EDT

The following was in the New York Times, June 13, 1989, p. B12:

Computer Glitch is Costly

Bettors who had the early daily-double yesterday at Belmont Park were supposed to get back about \$70 for hooking up Dyna Mite Mollie in the first race with Jazz City in the Second. But a computer glitch knocked their payoff down to \$3.40 and made winners out of everyone who had picked the winner of the first race.

A defective computer file knocked out the track's parimutuel system after the first race, and track stewards ordered the second race to be run a as non-betting event after first delaying it for 27 minutes. Under State Racing and Wagering Board rules, all bets on a non-betting race must be refunded, and the non-betting race must be removed from multiple-race bets involving it.

So track officials had no choice but to pay off a consolation daily double of Dyna Mite Mollie in the first and ``all'' in the second. Actually, the \$3.40 payout on the ``4-all'' combination turned out to be a bit more profitable than betting on Dyna Mite Mollie to win. She paid only \$3.20.

The computer problem was resolved after 55 minutes, and the remaining races were run without any problem. The cancellation of the other second-race bets prompted a statewide refund of \$439,144.

Rick Zaccone

### Commercial Loans in California at a Standstill

Peter G. Neumann <Neumann@KL.SRI.COM> Wed, 14 Jun 89 14:04:28 PDT

A new \$4.1 million computer system designed to enable recording, indexing, and scanning of 5.5 million pages of Uniform Commercial Code Division data was supposed to provide the equivalent of a title search for commercial borrowers in two days instead of two weeks. The new system went on-line on 5 April, but worked at only 30% of capacity. For every day's work, the

staff was falling 2.5 days behind. On 17 May they resorted to manual methods. The current backlog is 50,000 requests, and is not expected to be eliminated until 1 August. (The office is borrowing 100 employees.) Because of the enormous delays now encountered, many lenders have simply given up making commercial loans. (The contractor had urged the state to keep the old semi-manual system running as a backup, but the state apparently insisted on a cutover without retaining the backup.) [Source: abstracted from an article by Kenneth Howe in the San Francisco Chronicle, 14 June 1989, p. 1.]

### Phone Hacking

Brinton Cooper <abc@BRL.MIL> Tue, 13 Jun 89 8:22:44 EDT

From the Baltimore Sun, 13 June 1989, presented w/o permission:

Callers trying to dial a probation office in Delray Beach, Fla, yesterday heard sex talk from a panting woman named Tina instead. [...named Tina instead of what?...]

Southern Bell officials said that a computer hacker reprogrammed their equipment over the weekend, routing overflow calls intended for the local probation office to a New York-based phone sex line.

They said it was the first time their switching equipment had ever been reprogrammed by an outside computer intruder...

The implications of a computer breach are staggering for phone companies. Intercepting corporate communications, uncovering unlisted telephone numbers and tampering with billing information all are plausible consequences of such computer security breaches.

I find it interesting that two of the three "implications" of such activity are inconvenient for corporations while one deals with personal issues. Unmentioned are the more insidious implication of this specific activity, rerouting incoming calls. Calls to 911, for medical care, or to a neighbor to come for help may be more costly in human terms than "intercepting corporate communications."

Brint

#### Microcomputers in the operating theatre

Martyn Thomas <mct@praxis.UUCP> Tue, 13 Jun 89 12:45:23 BST

This article appears in the July 1989 issue of Micro User (a hobby computing magazine). I have written to the named anaesthetist to persuade him to think again, and to the magazine to explain the problem. I must emphasise that I have no direct knowledge that the report is true, which is why I have suppressed the name of the anaesthetist. The problem remains, though. How

can we spread understanding of the problems of using computers in safety-related applications, and of the minimum set of techniques which should be employed if such systems are being developed?

{ A BBC Micro in the operating theatre

Anaesthesia is a precise art and at University Hospital, Nottingham [UK] there are moves to sharpen that precision by taking a BBC micro into the operating theatre.

... consultant anaesthetist [name given] plans to connect the machine to syringe drivers and so improve control over drugs given to patients during operations. Senior lecturer at the hospital's adjoining medical school, he hopes to take this even further by using the micro to receive messages from the patient's body, adjust drug output accordingly and even act as a hazard warning for theatre staff.

As well as being put into practice during operations, his ideas will be used for teaching students in the Department of Anaesthesia.

"I am generally interested in looking at micro applications in the operating theatre", he told Micro User. "The first is to link up a micro to drive stepper motors and syringe drives which could get over the inertia problems of the linear motors which are used at present". }

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK. Tel: +44-225-444700. Email: ...!uunet!mcvax!ukc!praxis!mct

#### Inspiration from the past

Curtis Galloway <curtisg@sco.COM> Tue, 13 Jun 89 16:41:38 PDT

Whenever my faith in technology flags, I turn to my favorite source of inspiration: \_The Wonderland of Tomorrow\_, by Jean Carper. I thought I would share some of its prophetic words with RISKS readers. (I particularly like this chapter's title; I only wish I could send along the illustrations.)

Copyright Albert Whitman & Co., 1961. Reproduced without permission.

Chapter 3

Machines Will Take Over

The electronic computer is the most marvelous machine ever invented. It is often called the electronic "brain" because it does work so fast and accurately. It has been widely used for only about ten years, yet it has already changed our lives.

Some day a computer will run an entire company. It will make about sales, production and personnel that are much more accurate

than decisions made by businessmen. Companies already have employed computers to determine policies.

One day doctors may use computers to determine what is wrong with their patients. The doctor will feed a list of symptoms into a machine, and it will tell him exactly which disease he should treat. In an experiment at Cornell University a computer and a doctor diagnosed the ailments of 350 people, and the computer did a better job than the doctor.

Airplanes without human pilots may soon fly passengers and freight across the country. Air traffic will be controlled from the ground by computers. Some airports are now using computers to help prevent mid-air collisions.

Computers already have translated Russian books, speeches, and scientific papers into English. So far, these machine translations are crude and imperfect, but improvements are made all the time. Soon we may see translations of hundreds of foreign books and magazines in any bookstore. It will be possible because computers made the translations many times aster than human language experts could. How rapidly new ideas will travel!

- [...] People who work with computers sometimes call them "idiots." A man, called a programmer, has to tell the machine how to work problems step-by-step. He feeds instructions into the machine, and each time the machine works a problem it must consult the instructions. This series of directions is called a program. A program is so somplicated that a man may sped several months developing it.
- [...] A prominent scientist has suggested that we eliminate wars by having the generals of unfriendly countries play war on the computer. No lives would be lost, and no cities destroyed. The generals of each country would simply feed their battle plans into the computer. The machine would run through the battles and show which side won. The losing country could perhaps pay a fine to the winner, and everyone would continue living peacefully.

We have seen very little of what computers can do, but we can expect amazing things of them. One day the development of the computer may be regarded as a greater achievement than smashing the atom!

Curtis Galloway -- The Santa Cruz Operation, Inc.

#### "Illuminatus!" (Brunnstein, Wily hackers, RISKS-8.77)

<pete@basser.cs.su.OZ.AU>
Wed, 14 Jun 89 19:16:16 +1000

I believe that the book in question must be "Illuminatus!" by Harold Shea and

Robert Anton Wilson. The book is a spoof on conspiracy theories, and intimates that many and probably all human institutions are just fronts for a small group of 'enlightened ones', who are themselves a front for the Time dwarves of Reticuli Zeta, or perhaps Atlantean Adepts, remnants of Crowley's Golden Dawn, or even more likely the Lloigor of H.P. Lovecraft's Cthulhu Mythos. A leading character in this book is named Hagbard Celine.

"Illuminatus!" is a fun read if you like psychedelia and paranoia. It also seems to have influenced a lot of subsequent work, most notably Adams' "Hitchhiker's Guide to the Universe". It is easy to see how an unbalanced mind, taking it literally, could be completely absorbed. In fact "Illuminatus!" purports to intend just this sort of programming, referring to it as 'Operation Mindf\*\*k'. I don't think this constitutes a real danger for the vast majority of sane adults, but it may, tragically, have been the case here. Or perhaps, no disrepect intended, Koch may in the course of various hacks really have discovered too much about the Illuminati. After all, they are supposed to be the secret power behind the KGB ...:-)

(pete%basser.oz.AU@UUNET.UU.NET){uunet,mcvax,ukc,nttlab}!munnari!basser.oz!pete JANET: (POST) pete%au.oz.basser@EAN-RELAY (MAIL) EAN%"pete@au.oz.basser"

#### ✓ Praise and Blame -- Computers and People

Hugh Miller <MILLER@vm.epas.utoronto.ca> Tue, 13 Jun 89 10:29:24 EDT

Michael Doob ("The Computer Didn't Commit the Crime," <u>RISKS 8.78</u>) remarked that his bank has taken to citing "human error" instead of "computer error" when apportioning blame for mistakes. This is, of course, getting to be a familiar pattern to RISKS users (e.g. the Airbus crash, the Vincennes, etc.). Two things are worth mentioning:

- (1) In the case of big systems, the investment grows so great and becomes such a milk-cow for so many people and institutions that any scapegoat but the system itself will do in the event of a breakdown. The irony in this lies in the fact that the charge of "human error" is correct, in a way: we humans erred in constructing a buggy system and regarding it as reliable.
- (2) We used to cite "computer error" because it was a convenient way to deflect blame away from human persons. Implicit in this behaviour was a view that human persons possessed a moral dignity not proper to the machine, and that it was therefore better that the lower entity take the rap. Our new pattern of blame suggests that we have set this order of values on its head.

Hugh Miller, University of Toronto

✓ NORAD Computers: Years Late, Unusably Slow, \$207 Million Over Budget

Karl Lehenbauer <karl@sugar.hackercorp.com> 13 Jun 89 04:59:00 GMT

Two major new North American Aerospace Defense Command computer systems have encountered software development problems that have increased costs by at least \$207 million dollars and will be at least seven years late when delivered.

According to Aviation Week and Space Technology (May 22, 1989, pp. 24 & 25), the Space Defense Operations Center (SPADOC) modernization and the Communications System Segment Replacement (CSSR) programs, both part of the Cheyenne Mountain upgrade at Colorado Springs, have encountered major delays in their development, prompting criticism of the management of both programs from the General Accounting Office (GAO).

The GAO report criticized the project for its unrealistic expectations and the willingness to start the second phase before the first phase had been completed. The commander of the U. S. Space Command, USAF General John Pitrowski, said that the reports are substantially correct, but he disagreed with certain of the GAO's recommendations.

SPADOC is the data processing and communications center that supports the North American Aerospace Defense Command. The center is supposed to be able to maintain information on the position of up to 10,000 man-made objects in space. It is also to provide warning of an attack, and to determine when satellites need to be maneuvered for their safety.

The SPADOC modernization program was divided into three blocks -- A, B and C. Full-scale development on Block A started in 1983 and was intended to provide the hardware and software to automatically monitor and assess foreign activities that might put U. S. satellites at risk. Block B is to have the ability to make predictions of the orbits of about 400 satellites, and to automate a space object database that catalogs about 10,000 objects. Finally, Block C is to add greater automation, and to provide for the growth requirements of the system through the year 2005.

The prime contractor is Ford Aerospace and Communications Corp. IBM is the major hardware supplier. Logicon, Inc. is providing independent validation and verification of the software for the Air Force, and the Mitre Corp. is providing engineering support to the Air Force as well. According to the GAO report, both Mitre and Logicon raised concerns about the quality of Ford's software development and whether Ford would be able to meet the schedule.

The Air Force accepted the Block A system, even though (according to the GAO) it did not satisfactorily perform 14 of 23 required functions within the specified time limits. One example is that notification that a satellite is under attack takes four times longer than specified. According to the article, Mitre reported that in tests conducted in 1988, the system was so slow that at several points it was almost impossible to interface with it through the operators' consoles. The software is unstable as well, and unacceptable times to restart the system after a problem had occurred (presumably software exceptions and such) were also cited.

Ford has proposed a new architecture for Block B using IBM 3090 computers. Ford also says that these computer will be sufficient to handle the Block C

portion as well.

The GAO also noted that, even if the software had worked and been on time, it could not have been installed in Cheyenne Mountain due to a lack of uniform wiring standards for computer and telecommunications equipment and congestion in the cabling area. Pitrowski agreed that the Air Force should have resolved the wiring problems sooner, but noted that the Air Force awarded a contract for facility modifications on April 19th.

Karl Lehenbauer



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 8: Issue 80

**Friday 16 June 1989** 

## **Contents**

Disarmament by defect

**Gerard Stafleu** 

Even human-in-the-loop isn't foolproof. A test case.

Pete Holzmann

Single point of failure? probably not.

**Ephraim Vishniac** 

Re: single point of failure -- Tokyo Stock Exchange

Patrick Wolfe

Qantas Airliner Mishap

John Murray

Theorem Proving by Computers

Tom Thomson

Re: Computer electrocutes chess player ...

**Dave Horsfall** 

Joel Kirsh

Clerical error spares famed sex-fiend

Mike Albaugh

Sabre computer problems revisited

Emily H. Lonsford

Protection from Misdirected Radio Control Commands

**Robert Horvitz** 

Info on RISKS (comp.risks)

#### Disarmament by defect

Gerard Stafleu < gerard@uwovax.uwo.ca> Thu, 15 Jun 89 11:00:29 edt

We have seen quite a few articles on things going wrong with the computerization of the military. The latest example is the posting by Karl Lehenbauer about "NORAD Computers: Years Late, Unusably Slow, \$207 Million Over Budget".

While most articles concerned the Western military, there is no doubt

that our friends on the other side suffer from the same problems. After all, they are doing their level best to get their hands on as much Western computer technology as possible. (I have heard rumors that getting our technology to them is one of the most subtle and insidious plots developed by the CIA so far.)

As a result, it is reasonable to suspect that the advance of computer technology into the field of the military, has made it well neigh impossible to fight any war worth its SALT. We find corroborating evidence for this position in the on-going disarmament proposals. These have been started by Gorbachov, who knows an impossible situation when he sees one, and have now been taken over by Western leaders like Bush, who perhaps reads comp.risks.

So where the sheer incompetence of politicians and generals used to start wars, the sheer incompetence of us computer people has now put an end to it. No mean feat. For centuries humanity has been looking for the Weapon That Would End War Forever. We have found it. War has ended, not with the bang of a bomb, but with the gentle whisper of crashing software.

Gerard Stafleu, (519) 661-2151 Ext. 6043 BITNET address: gerard@uwovax

## Even human-in-the-loop isn't foolproof. A test case.

Pete Holzmann <pete@slp.UUCP> Wed, 14 Jun 89 14:10:29 PST

I was recently witness to an event that may be of interest to those pondering safe user interfaces, man-in-the-loop questions, and the like. Not being an expert in any of these areas myself, the only comment I'll make is that it seems important to realize that there are cultural aspects of human-technology interfaces. Never assume that a sane, well-trained person will do 'the right thing'...

The following is a true story. No names are given, so as to protect the participants from any further embarassment!

The scenario: experienced computer user/programmer needs to get some software mailed out during the weekend. He's relatively new to the office, so he has asked where the spare floppies are kept. He is told "there's a box with a bunch of floppies over on Joe's desk". There's a small error in these instructions: the correct box of spare floppies is on Jane's desk, not Joe's.

What happens: He goes into the office alone on Saturday morning. Nobody is there to watch him (not that anybody normally would -- he's an expert, remember!) He finds no box of floppies on Joe's desk. But - aha! - there's a nice big box UNDER the desk. It is sealed. (It was delivered the day before.) He opens the box, and finds a bunch of brand-new commercial software packages. Shrink-wrapped, the whole bit. Without skipping a beat, he rips open a couple, and finds sealed white

envelopes inside. The envelopes have your usual dire license agreement warning, beginning with a large STOP sign... ("STOP. Read before opening! etc...") Without skipping a beat, he rips open the envelopes, reformats the enclosed floppies, puts on new labels, and uses them to mail the software he needed. Thus ruining a few thousand dollars worth of new commercial software!

Now, before you read the answer, think about this puzzle: how could a sane person, an \*expert\* no less, completely ignore the warnings and do such a crazy thing? What are the RISKS implications of this?

Here's the answer:

He was able to do it, without even wondering whether it was the right thing to do, because \*in his experience\*, what he saw and his resulting actions were completely normal. In a previous job, his company received large quantities of commercial software for evaluation and review. So much software that they treated it like junk mail. The floppies were treated as reusable media. With that in mind, his actions become completely reasonable! He was trained to ignore dire warnings, expensive-looking software packaging, and the like. The only thing of value in a box of commercial software, in his experience, was the floppy disks themselves. And they were only useful once reformatted and with fresh labels on them.

Hmmmmm...

Pete Holzmann, Strategic Locations Planning {hpda,pyramid}!octopus!slp!pete

#### ✓ single point of failure? probably not.

<ephraim@Think.COM>
Thu, 15 Jun 89 09:47:53 EDT

In <u>RISKS 8.79</u>, Jerry Carlin (jmc@PacBell.COM) cites a story from the SF Chronicle (presumably San Francisco, and not some 'zine):

The reporter quotes a story in "Manhattan, Inc" where it was disclosed that the main and backup computer for the Tokyo Stock Exchange sit right next to each other and in an area totally destroyed by the 1923 earthquake.

This computer is the SOLE repository of Japan's offical records of stock ownership. Therefore if the computer is destroyed, all records of share ownership could disappear with obvious consequences.

It seems very unlikely that the computer is the SOLE repository. More likely, the two computers together with the on-site and off-site backups of the data they contain are the widely distributed and highly redundant repository of the stock ownership data. That's not such an exciting story, of course.

Supposing that Tokyo Exchange follows conventional backup procedures (and they could easily do much better), destruction of both computers would mean the loss of the current day's transactions; destruction of the entire site might mean the loss of as much as one week's transactions. That's expensive, but it's not catastrophic.

Ephraim Vishniac, Thinking Machines Corporation, 245 First Street, Cambridge, MA 02142-1214

## ★ Re: single point of failure -- Tokyo Stock Exchange

Patrick Wolfe <pwolfe@kailand.kai.com> Thu, 15 Jun 89 07:27:26 cdt

- > This computer is the SOLE repository of Japan's offical records of stock
- > ownership. Therefore if the computer is destroyed, all records of share
- > ownership could disappear with obvious consequences.

This is why people in my position spend so much time with and are so concerned about backups, so that the computer is not the "SOLE respository" of any valuable information. Well managed computer centers keep a set of complete backups "offsite". The ones with larger budgets use an storage location complete with protection against fire and other environmental hazards.

The only story I have heard about a computer center that didn't keep any backups is about US Cable in Lake County, IL. Every six months or so, they would unscramble all six pay channels for everyone for about a week, reportedly because of a "computer problem" where they lost information about who was paying for which channels. If they had reliable backups, these records could have been restored in a matter of hours, instead of a week.

Patrick Wolfe (pat@kai.com, kailand!pat) System Manager, Kuck & Associates, Inc.

#### Qantas Airliner Mishap

John Murray <johnm@uts.amdahl.com> Thu, 15 Jun 89 17:30 PDT

I heard an NPR report recently about a Qantas plane going out of control temporarily. It seems the autopilot suffered some sort of glitch. The (human) pilot recovered from the dive, but several people bumped their heads, etc. Since then, I've heard no follow-up, and seen nothing in comp.risks.

Was I hallucinating about the original report, or do I just have my head in a bag this month??

- John Murray, Amdahl Corp.

#### Theorem Proving by Computers

Tom Thomson <tom@prg.oxford.ac.uk> Thu, 8 Jun 89 09:43:04 bst

Henry Spencer comments on the acceptance by mathematicians of proof by computer. I think it's important to recognise that the computer introduces no new risk here; we all believe group classification theorem, don't we, and surely no-one has ever found time to check the proofs (or even understand the underlying arguments) of all the lemmas and prior theorems involved therein.

Mathematics has a long history of "proofs" that aren't (eg the omission of axioms about betweenness in geometry for a couple of thousand years); and quite a few "theorems" have been disproved. Checking a proof is no easier than checking a program. Checking that several proofs combine correctly to deliver a new proof is no easier than checking that several programs combine correctly.

Do we have a new risk here - the risk that, because a computer is involved, we will assume a new risk exists even when it doesn't (or is not new)?

Tom Thomson

### ★ Re: Computer electrocutes chess player who beat it! (RISKS 8.75)

Dave Horsfall <munnari!stcns3.stc.oz.au!dave@uunet.UU.NET> Thu, 8 Jun 89 11:21:29 est

[ Discusses receiving a strong shock from a 12-volt wiper ]

More likely he received an inductive shock from the electric motor. There is no way that a mere 12 volts will cause that sensation, but a kick of a few hundred (thousand?) volts will do it, as the field collapses.

#### Computer electrocutes chess player

Joel Kirsh <KIRSH@UTORMED.bitnet> Thu, 1 Jun 89 21:51:00 EDT

[Excerpted, from "Bioengineering: Biomedical, Medical and Clinical Engineering", by A.T. Bahill (Prentice-Hall)]

The impedance of the human body can be modeled as a core of low resistance (around 500 Ohms) ... and the skin with a higher resistance (1 to 100 kiloOhms). ... the amount of electrical current necessary to induce venticular fibrillation [a "cardiac arrest"] in the human heart ... a minimum of 80 microAmps, 100 uA, and 180 uA [in three separate studies].

These values lead to estimates of the required voltage being anywhere from 240 mV (80uA times 3 kOhms) to 16 V (180 uA times 201 kOhms). Of course, this assumes that the current path crosses the chest. Also, the heart is especially susceptible to particular frequencies; good old 60 Hz is "the optimum frequency for producing ventricular fibrillation." (Bahill)

Joel Kirsh, Faculty of Medicine, University of Toronto

#### Clerical error spares famed sex-fiend

Mike Albaugh <albaugh@dms.UUCP> Wed May 31 10:54:17 1989

Quoting from Colin Wilson's "The Misfits":

The revolutionary Marat decided that de Sade was a typical aristocratic libertine of the old regime and ought to die; by accident, however, he denounced the Marquis de la Salle, who was executed. Marat discovered his mistake and was about to rectify it when he was murdered in his bath by Charlotte Corday. Unaware of how close he had been to the guillotine, de Sade delivered an address describing Marat as a great man.

The parallels to modern wrongful arrest struck me, as well as the question of how bad the reign of terror might have been with the "help" of modern data processing. It appears the over-reliance on the accuracy of "official" orders has been around for a while. Perhaps Madame DeFarge should have used an error-correcting code in her knitting?

[My remembrance of early dp is that redundancy in the form of hash totals and transaction serial numbers was used quite early, and seems to have been forgotten, rather than enhanced, as we have "advanced"]

Mike

## Sabre computer problems revisited

Emily H. Lonsford <m19940@mwvm.mitre.org> Tuesday, 30 May 1989 10:01:46 EST

According to the May 22, 1989 issue of Computerworld, Sabre is run on 8 interconnected 3090-200E computers under a Sabre-modified version of ACP (Airline Control Program OS by IBM). A custom version of ACP has been used there for about 20 years. Neither ACP nor TPF 3.1 (due to be installed 3rd qtr 89) provides the required protection, according to the article. It seems the errant 'core-walker' program modified another task that was formatting disk drives - and the labels on 1080 disk drives were destroyed.

"The Sabre system is down an average of six minutes a week for maintenance, Juracek noted, and is usually upgraded 'on the fly' so that service to other parts of the world is not disrupted. Because ACP cannot run without a disk subsystem, Sabre software engineers took the unusual step of rebooting the crashed system using IBM's VM operating system. Then, they had to relabel each disk drive and reset the pointers that indicate where passenger data is located....While most Sabre data was not lost, the 'pointers' to all flight reservation data were - and it took 100 programmers and systems engineers more than 10 hours to relabel each disk volume. The system was restarted under ACP about 7 am CDT, and the reformatting was done by 11 am. Then, due to pent-up network

demand, American's systems engineers had to gradually restart Sabre, slowly admitting more traffic from 27 front-end communications processors here."

ACP and TPF are IBM real-time operating systems that are designed to support heavy transaction volumes. The article goes on to state that virtual storage will not be available under TPF until 1993. Apparently other protection features are not there either, such as private address spaces and multiple storage protection keys, which are implemented under MVS.

Emily H. Lonsford, MITRE - Houston W123 (713) 333-0922

#### Protection from Misdirected Radio Control Commands

Robert Horvitz <rh%well%apple@sun.UUCP> Fri, 2 Jun 89 00:45:43 pdt

In <u>RISKS 8.75</u>, MIchael Berkley quoted a newspaper article about an accident in northern Ontario in which a radio-control signal intended for one mining machine triggered an unintended response in a second machine, which pushed a miner to his death. Berkley asked: "What kind of safeguards are possible in this situation and are the safeguards reliable?"

I am not familiar with Canadian regulations for radio control, but they are probably similar to US regulations. As it happens, the FCC has just adopted new rules governing radio signals from unlicensed devices, including radio control systems (Gen. Docket 87-389: First Report & Order adopted 30 March 1989). The Commission is explicitly trying to encourage the proliferation of low-power unlicensed radio devices of all types, in the spirit of "deregulation" promoted by outgoing FCC Chairman Dennis Patrick. The primary feature of the new "Part 15" rules is to loosen restrictions on the use of radio links in appliances and systems sold publicly. The new rules begin to take effect on June 23rd. They are sure to lead quickly to a rash of new products such as wireless modems, wireless VCR/camera units, new remote monitoring and control systems for the home, etc. One aspect of the new rules relevant to the mining story is that the FCC set no maximum power limit for radio emissions in mines, caves or tunnels.

A traditional feature of all "Part 15" devices is that they enjoy no right of protection from interference - either from similar devices or from licensed transmitters. Licensing confers the right of non-interference. Radio control systems are generally unlicensed.

Since most of the services that the Commission regulates are for communication, they are used to thinking of interference in terms of, e.g., degradation of TV picture quality. They are not used to thinking of it in terms of misdirected control. In fact, because Part 15 devices have no recognized right of non-interference, the Commission's attitude is - and has always been - "buyer beware/you're on your own."

Thus, the only safeguards we can expect in the US, to avoid accidents like the one that killed the Canadian miner, are those voluntarily adopted by manufacturers. Fortunately, there is a relatively simple fix to the problem:

have each radio command begin with an identifier specifying which device is being addressed, and have the identifier be unique enough that there is little chance of two devices with the same identifier being co-located. Better, have the owner or operator be able to set the identifiers in the field, to ensure each is unique within the transmitted signal's radius.

Over a dozen petitions have already been filed objecting to the FCC's new rules. I will probably be filing comments soon on behalf of the Association of North American Radio Clubs. I may raise this issue of radio control safety in my filing. But I'm sure the Commission will say that this is a matter for the marketplace can decide, and no "interference" from them is needed.



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 8: Issue 81

Saturday 17 June 1989

## Contents

Re: Disarmament by defect

**Gary Chapman** 

Medical history-on-a-card?

Ellen Keyne Seebacher

No backups -- TOWER of Babel

Sam Cramer

'Blip' Blows Computers Back to Paper Age

Mark Osbourne

Re: Computer electrocutes chess player who beat it!

O. Crepin-Leblond

Re: Hartford Coliseum

Richard S. D'Ippolito

Info on RISKS (comp.risks)

## Re: Disarmament by defect

Gary Chapman <chapman@csli.Stanford.EDU> Fri, 16 Jun 89 13:49:57 PDT

The plot of the latest John LeCarre novel, \*Russia House\*, involves a Soviet physicist who goes by the code name Goethe, who, in the story, was for many years in charge of the Soviet ICBM testing program, and created the telemetry encryption schemes that the Americans had been trying to break for many years (telemetry encryption is a serious dispute between the U.S. and the Soviets in real life). Goethe has an attack of conscience, and decides to reveal to the West that Soviet ICBMs are virtually duds--if they get out of their silos at all, they're just as likely to hit Minsk as Chicago. All of contemporary U.S. strategic theory, and strategic spending (hardened silos, SDI, launch-on-warning, etc.), is of course based on the assumption that Soviet missiles can fly right down the silos of Minuteman IIIs and MXs over here.

The interesting part of this story is the effect that Goethe's information has on U.S. authorities. The defense contractors go ballistic, if you'll pardon the pun. Their whole raison d'etre is based on continuing technological

refinement to counter a Soviet threat that is suddenly no longer there. The "Bluebird" documents (Goethe's notebooks) also call into question the whole multi-billion dollar apparatus of U.S. surveillance and intelligence analysis in the strategic arena--satellites, listening posts, KC-135s, trawlers, etc., not to mention brigades of experts. And the implication is that the U.S. arsenal is really no better, that we've all been living with the colossal implications of two enormous nuclear arsenals, and in actual fact neither one really works at all.

The result of this revelation from Goethe is largely just an escalation of the current stalemate between doves and hawks. The hawks claim Goethe's information is sophisticated disinformation, and if the information is deliberate disinformation then the claims of Soviet incompetence \*must\* mean that the missiles are actually even \*more\* accurate than we suspect. The doves claim that the information is accurate, and that there is no rationale for extravagant weapons systems that are supposed to protect us from a threat that has always been a hoax. This debate produces paralysis.

It would seem to me that technologists and scientists, contemplating the awesome significance of the integrated nuclear system that we live with every day, would want to know, objectively, whether the damn thing will work when it is called upon. Once this fact had been established one way or another, it would be immensely easier to grasp what sort of problems we face that can be bracketed out from the technological uncertainty that saturates the whole nuclear system. But, since a "test" of nuclear war is impossible--or at least so wildly crazy that no sane person would propose it seriously--we have an enormous, fundamental precedent for building other technological systems that have great risk, that cannot be tested, that are inseparable from political persuasions and irrational faiths, and which incrementally add momentum and depth to this process of scientific and technological corruption. Goethe suggests that when his scientific notebooks are published, they be titled "The Biggest Lie Ever," or something like that. But even Le Carre doesn't seem to realize how big the lie really may be--it may no longer be confined to nuclear weapons, but in fact may be endemic in a whole host of technologies that have been generated within the same, now one-dimensional epistemology of modern engineering--"we hope it will work; if it doesn't get back to us."

-- Gary Chapman, Computer Professionals for Social Responsibility

## 

"Ellen Keyne Seebacher" <see1@tank.uchicago.edu> Fri, 16 Jun 89 16:02:38 CDT

The following item appeared in SELF magazine (aimed at younger working women) a couple of months ago, and I've heard nothing about it since:

"Credit-card-size medical records are being used in several pilot programs in the U.S., and the British government is thinking about issuing them to the entire population. The pocket-sized plastic "smartcard" has a thin computer chip that stores basic info. -- blood type, allergies, current health and prescriptions -- plus a summary of

.)

insurance coverage. Down the road: "optical memory cards" using laser technology similar to compact discs. These could store a person's entire medical history from birth to death, including diagnoses from every visit to a doctor. The card could even plug into a computer to produce the patient's X-rays on a TV screen."

The technology under discussion here was not entirely clear: a "thin computer chip" -- like that in a calculator? How would this be read/written to? (A friend has told me that

when media ignorami use the words "computer chips", they could mean just about anything. In the context of "smart cards" they do in fact mean a tiny CPU and some memory, with electrical contacts on the card.

I had initial visions of people carrying their medical records around next to their ATM cards, with the same results -- like scrambling due to magnetic wallet clasps. The problems of storing an "entire medical history" on a card are even worse: lost cards, thefts, and invasion of privacy on a mass scale. Is this a naive assessment of RISK?

(I'm really interested in this. Would anyone with "smart card" experience care to comment?)

Ellen Keyne Seebacher, Academic and Public Computing, Univ. of Chicago

#### No backups -- TOWER of Babel

Sam Cramer <cramer@Sun.COM> Fri, 16 Jun 89 14:28:16 PDT

Another example of not keeping back-ups: I went into Tower Video about 6 weeks ago, selected a tape to rent, and presented the cashier with my Tower Video card. He told me that he'd have to issue me a new card number, as the old database had been wiped out in a crash. Tower is a chain; this loss of data was evidently company-wide.

I guess prospective Supreme Court justices should rent from Tower! Sam

#### ✓ 'Blip' Blows Computers Back to Paper Age

Mark Osbourne <osbourma@asd.wpafb.af.mil> Fri Jun 16 08:59:56 1989

Dayton Daily News - Tuesday June 13, 1989 Page 3

Office workers, police dispatchers and bank customers got a little taste of what life would be like without computers Monday when systems across Montgomery County crashed all at once because of a little electrical "blip".

A power failure of less than a second caused lights merely to flicker, but was enough to trip circuit breakers in some buildings and zap scores of computer systems into temporary chaos.

The county's new 911 computer-aided police and fire dispatch system was affected, delaying response time on some calls.

"It tool down the county's mainframe (computer)," said Sgt. Richard Elsner, 911 coordinator for the Montgomery County sheriff's office. "We had calls lined up in the computer waiting to be dispatched, and we just lost everything. Fortunately, we didn't have any emergency callers waiting."

Dayton Power and Light Co. spokeswoman Ethel Washington said the utility was unsure what caused the power failure, which she called a "blip." She said that "with something that quick, we may never know."

The lights flickered in the sheriff's dispatch center in the basement of the Montgomery County Jail at 11:18 a.m., Elsner said. "The lights went off for less than a second - I thought somebody cut across the lines or something," he said.

A second momentary pulse occurred about 11:30 a.m., he said.

The computer failure scrambled things for a few hours, but crews were dispatched as they were before the computer system was installed. "The radios are still working," Elsner said.

Washington said DP&L's computers in the West Dayton office, from which she was calling also were down.

For reasons of security, many private users were mum about the power failure's effect on their computer systems, "It was nothing major," Society Bank spokeswoman Susan Byers said.

Nevertheless, customers at several banks were unable to make transactions at automatic teller machines until the mess was straightened out.

Tina Hamden, general manager of All World Travel, said airline reservation computers at the downtown office shut off automatically when the power went down. Office telephones went dead as well, leaving clients hanging.

The travel agency did not lose any computer data, but a local computer expert said that is a risk for most computer users.

If a computer user is accessing data using a disk drive, hard disk or other storage device during a power failure, that data may be lost during the transfer from the storage device to the computer's internal memory.

"It goes to that nebulous void for computer data," said Robert Stamper, president of Databank Information Services Inc., a Dayton company that provides emergency services for computer users.

"If you don't have a backup, you have to re-enter that data - it has to be keyboarded back in all over again, and on a big computer, that can cost an absolute fortune."

Stamper said his staffers were kept busy Monday afternoon delivering backup copies of computer tapes to clients who lost data during the power failure.

"They're calling us saying, 'Bring the tapes back out,'" Stamper said.
"They either need a section of their computer records or need to reconstruct their lost data. If that was a blip, that was a hell of a blip."

His customers, which include several large area companies, were also reluctant to discuss problems that arose with their mainframe computers.

"They don't want people to know how vulnerable their systems are," Stamper said.

## Re: Computer electrocutes chess player who beat it!

<ZDEE699@elm.cc.kcl.ac.uk> 16-JUN-1989 16:56:11 GMT

In <u>RISKS-8.75</u>, Gene Spafford (spaf@cs.purdue.edu) writes about the Soviet computer which zapped his opponent when the opponent was about to beat him... Some may say this is bogus... but it is in fact perfectly possible.

According to the message, this is no normal computer. It is dedicated to playing chess and moves its pieces on the chess board. This is possible by magnetising the chess pieces, and moving them by induced electromagnetic fields in the board. The fields are induced by passing a current through loops and coils of wires which are embedded in the board. This is all to tell you that it is possible for the machine in question to use high voltages. Alternating current is no use for producing the magnetic fields wanted, so I suspect they used DC... and DC currents are LETHAL. The muscles contract when the current flows so the heart of the player would stop immediately. So one only needs a short circuit to the case of the chess board (which I suspect was made of metal and not well earthed) and the friendly computer can become a murderer.

O. Crepin-Leblond, Computer Systems & Electronics, Electrical & Electronic Engineering, King's College London, UK. Disclaimers: the usual disclaimers apply...

## Re: Hartford Coliseum

<rsd@SEI.CMU.EDU> Thu, 15 Jun 89 17:03:24 EDT

[Rich contributed an item which I ran in Software Engineering Notes

four years ago. Here is a fuller explanation. PGN]

In the early morning hours of January 18, 1978, a very heavy load snow and ice from a winter storm caused the collapse of the 2.4 acre roof of the Hartford Coliseum in Hartford, Connecticut. This roof was noted for being one of the first large-span roofs made possible by computer design and analysis, and was modeled as a space truss using a trusted program. Fortunately, the several thousand fans attending a basketball game a few hours before had gone home, and the structure was empty.

After long analysis of the collapsed roof, the initial failure was found to have occurred in a lateral brace used to stabilize a long, slender truss member. The immediate cause of failure was the inadequate design of the connection of the brace. The joint was modeled in the computer as having no eccentricity, an incorrect assumption. Eccentricity in a connection means (briefly) that the axis of the applied load is not the same as the neutral axis of the support, so that a bending moment is developed, putting additional stress in the member.

A nonlinear collapse similuation was rerun using the correct model for the joint, and with loading conditions selected to approximate those of the night of failure. The result was that the connection failed as it had under the real conditions [1].

Quite simply, the problem here was: The structure analyzed was not the structure built.

[1] Hartford Roof Failure -- Can we Blame the Computer? Epstein and Smith, Proceedings, Seventh Conference on Electrical Computation, 1979.

Rich



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 8: Issue 82

Monday 19 June 1989

## **Contents**

Re: Microcomputers in the operating theatre

**Ken Howard** 

Risks of missiles

Steve Den Beste

Trojan Horse in Comp.Risks?

John C Williams

Power glitches scrambling computers --- can it be avoided?

Will Dickson

Re: 'Blip' Blows Computers Back to Paper Age

William M. Bumgarner

No back-ups: Ninth Circuit's "computer error"

**Clifford Johnson** 

Hillsborough Football -- Another Computer Connection

**Charles Lindsey** 

Radio Control Interference

Marco C. Barbarisi

New Yorker Article (book serialization?) on radiation risks

Martin Minow

Info on RISKS (comp.risks)

## ★ Re: Microcomputers in the operating theatre (RISKS-8.79)

Ken Howard <khoward@chook.ua.oz.au> 19 Jun 89 05:05:38 GMT

In RISKS-8.79, Martyn Thomas says:-

- > Anaesthesia is a precise art and at University Hospital, Nottingham [UK]
- > there are moves to sharpen that precision by taking a BBC micro into the
- > operating theatre.
- > .... consultant anaesthetist [name given] plans to connect the machine to
- > syringe drivers and so improve control over drugs given to patients during
- > operations. ...

Martyn addresses the obvious risk from the hardware/software reliability point of view here. The other not so obvious risk is that a BBC micro is not certified for use in an environment containing explosive gasses such as are used in anesthesia ....

You could switch the machine on/off and .... [consequences left to the reader's imagination!]

---Ken---

Ken Howard, University of Adelaide, Dept. of Computer Science, G.P.O. Box 498, Adelaide 5001 AUSTRALIA.

#### Risks of missiles

<denbeste@BBN.COM>
Mon, 19 Jun 89 10:47:28 -0400

With regard to the Minuteman system, the system is guided only in the sense that you may preprogram it for any destination. It is NOT self-correcting on its course. The main missile is solid fuel, which means that once you light it off, it will burn until it's gone (like the SRB's on the shuttle). They can control the direction of the thrust but not its intensity.

At this point it is gliding until it releases its warheads. The missile has no mechanism for sensing where it is and aiming the warheads accordingly - it is just told, BEFORE LAUNCH, "point here, release a warhead, point there, release a warhead, etc." The point is that all errors in the launch are cumulative and no mechanisms exist to correct them.

Which makes the following very important: All tests of the Minuteman, and there haven't been very many, have been from Vandenberg AF base in CA, aimed at an atoll in the south Pacific. The missiles rise out of the atmosphere, but never enter the Van Allen belt.

The Van Allen belt, like any magnetic field, is a toroid, and if a Minuteman was really fired it would be over the pole - and it would pass through the Van Allen belt twice. It is also the case that the local gravitation field characteristics over the pole are different than they are over the Pacific.

None of this matters much when you are shooting at something like a city which is miles across. It matters a great deal when you are shooting at a hardened target like a silo or a bunker. There an error of 100 yards is the difference between success and failure in knocking out the enemy target.

If the last war does happen (let's hope not) there is no question that our Minuteman force can destroy all the cities in the USSR. To use them in a first-strike against silos, on the other hand, is a crapshoot. (If anything, the situation from a Trident is even worse because your starting position may not be known completely accurately.)

I suspect that those in charge of our nuclear forces know this, and it is one of the reasons we haven't had the war (though hopefully not the only one).

This reminds me of another story, equally interesting: Shortly after coming to office, the Reagan administration asked the Soviets to destroy a certain class of medium range missiles in Europe in exchange for a promise from us not to develop an equivalent one. The Soviets laughed.

So we developed the Pershing II. It was only tested twice, and it blew up during launch both times.

...at which point, the powers that be said "That's good enough. Deploy it." So we built over a hundred of them and put them in Germany and the Netherlands (political disturbances and picketing notwithstanding).

Ultimately they were traded for the Soviet equivalent class in the INF treaty. It makes you wonder whether the Pershing II ever had any other purpose, doesn't it?

Steven Den Beste, BBN Communication Corporation, Cambridge MA

## Trojan Horse in Comp.Risks?

John C Williams <jcw@wdl1.fac.ford.com> Mon, 19 Jun 89 12:52:55 PDT

A contributor to Comp. Risks 8.80 (Disarmament by defect) suggests "... that the advance of computer technology into the field of the military, has made it well neigh impossible to fight any war worth its SALT."

(Emphasis added.)

Is this an example of a Trojan Horse?

John C. Williams, Ford Aerospace

[The "neighs" have it. A "Nigh" for a "nigh". Note that NYACK (NY) must be NEARLY an ACKnowledgement. PGN]

# Power glitches scrambling computers --- can it be avoided?

Will Dickson <will@robots.oxford.ac.uk> Mon, 19 Jun 89 11:43:50 BST

Several recent articles in RISKS have mentioned computer failures due to various glitches on the power supply lines. At the same time, many companies are advertising Uninterruptible Power Supplies (UPS's) claiming that they safeguard against these problems, or at least that they provide enough time for a graceful shutdown in the event of a power failure.

What is the actual situation? Are these UPS's capable of doing what they claim? If so are they not used because of the cost, or because people do not feel that they are needed? Or are there other issues?

Will Dickson.

Robotics Research Group, Department of Engineering Science, Oxford University, Oxford OX1 3PJ, England.

JANET: will@uk.ac.ox.robots

## Re: 'Blip' Blows Computers Back to Paper Age

"William M. Bumgarner" <wb1j+@andrew.cmu.edu> Sun, 18 Jun 89 19:19:30 -0400 (EDT)

A momentary electrical 'blip' is a dangerous thing; I lost my computer to one this morning.

Last night, there was an electrical storm in the area-- no close strikes or power problems. But this morning (clear skies), i heard a crack/ explosion like a transformer blowing out. Immediately following this was a momentary (less than one second) loss of power. Later, when I went to use the computer (Mac Plus w/a flaky video board anyway), the video had been reduced to a 3 millimeter wide strip up the middle of the screen (Horizontal scan gone?) Whether or not the storm had any connection with the 'blip' is questionable, but the blip definitely nailed my computer.

BTW: the logic board is fine... only the video was lost.

Questions: What is the best way to protect against a blip (UPS? isolation transformer?)?

What measures have been taken to protect against such blips in critical systems? How much of a threat are 'blips' to hardware?

b.bum wb1j+@andrew.cmu.edu

## ✓ No back-ups: Ninth Circuit's "computer error"

"Clifford Johnson" <GA.CJJ@Forsythe.Stanford.EDU> Sun, 18 Jun 89 11:14:21 PDT

After an oral hearing in the appeal of my old lawsuit (re launch on warning and the question as to whether that capability delegates a decision to declare war to the military and its computers), I asked for a transcript of the hearing. I was told over the phone that it had been located and would be transcribed, but then received a form stating, without apology or explanation, that it was "unavailable." I asked why this was the case, on the phone to the clerk, and was transferred to someone who told me that the transcript was not available due to "computer error."

She explained that only in the past few months (\*"this year"\*) had the taping of hearings become the procedure, that my tape had mysteriously disappeared ("probably someone with access didn't want it published", she supposed), and that this loss had caused the court (Ninth Circuit court of appeal, San Francisco) to

realise for the first time the need for back-up tapes.

Accordingly, procedures had been changed so that originals would be kept securely henceforth, she stated, pleading that it was ignorance of the new computer (tape-recorder = computer in her books) technology that caused the problem.

However, there was no problem finding the tape of a hearing I had in the same court some \*three years\* earlier.



Date: Mon, 19 Jun 89 15:27:43 +0100

From: Charles Lindsey <charles@unix.computer-science.manchester.ac.uk>

Subject: Hillsborough Football -- Another Computer Connection

In the UK, we recently had a major disaster at the Hillsborough football ground in Sheffield, in which 95 people died after being crushed against the steel barrier which is supposed to prevent the spectators from invading the pitch. It is estimated that the pressure per person on the fence, due to the weight of the people behind surging forward, was in excess of one ton.

[The computerized turnstile problem was noted in RISKS-8.60. PGN]

Now the official enquiry into the disaster is sitting, and the papers are full of reports. At some point, it seems the Police decided they needed cutting gear to use on the fence, and telephoned the Fire Brigade for it to be sent. Clearly, its need was EXTREMELY URGENT.

Note that Hillsborough is the major football ground in Sheffield. It must occupy something the size of a city block, and it can be approached from several roads. The following is quoted from the Daily Mail for June 14.

Two vital minutes were wasted in helping victims of the Hillsborough tragedy.

The fire brigade refused to send vital cutting gear until they knew what street the football stadium was in. Four times telephone operator Susan Davies demanded the address. Then she asked five times what the equipment was needed for.

Yesterday Miss Davies told the enquiry ... that the fire service computer would not recognise the Hillsborough ground as a place.

'It needs a specific address and district in order to determine what pumps are required to attend', she explained.

'My training is not to assume what an address is. It's up to me to ascertain that from the person calling'. As far as she was concerned, she added, there could have been several football grounds at Hillsborough. ... The conversation ... went like this:

Police: Can we have cutting gear for Hillsborough please straight away?

Fire: Just a minute. Right, what's the address?

Police: Cutting equipment for Hillsborough football ground straight away.

Fire: Hillsborough football ground?

Police: Yes, Hillsborough football ground.

Fire: What road is that on, do you know?

Police: There has been a major accident, all the ambulances are there.

Fire: What road is it on?

Police: I have no idea. Hillsborough football ground.

Fire: What road is it on, do you know?

Police: Hillsborough football ground, what road is it on? (this to someone in

police control). Penistone Road.

Fire: Penistone Road?

Police: Penistone Road, OK.

Fire: Penistone Road, just a minute. What's exactly involved?

Police: It's football, a big match, Liverpool v Nottingham Forest.

Fire: Yes, but why do you want us? You said it was an RTA (Road Traffic

Accident).

Police: No, major incident inside the ground.

Fire: Major incident inside. Do you know exactly what it is?

Police: No I don't. They want all the cutting gear.

Fire: For what, do you know?

Police: Hang on a sec.

Police: (another voice) Hello.

Fire: Hello, now you want some cutting gear. What exactly is it for?

Police: ... full explanation ...

Fire: Right. OK. Leave it with us.

✓ Radio Control Interference (Re: RISKS 8.75 and 8.80)

Barbarisi <marco@ncsc.navy.mil> Mon, 19 Jun 89 14:53:17 CDT Micheal Berkley recently (RISKS 8.75) described a now infamous accident in which a radio controlled mining machine killed a man after receiving an interfering signal. In RISKS 8.80, Robert Horvitz suggested a possible fix in which the transmitter command is headed by a coded signal recognizable only by the receiver. Radio sets are readily available which feature pulse code modulation (PCM) and employ a header code ("password", if you prefer). They are commonly used to control model aircraft.

If a spurious signal interferes with a PCM receiver, it goes into a preprogrammed "failsafe" mode until contact with the matching transmitter is restored. The user usually has at least some control over what happens during failsafe mode. The default for most airplane systems is to neutralize (i.e., return to a center position) all control servos. Hopefully, this results in neutralized control surfaces and a 1/2 throttle setting on the engine. Of course, if the airplane is pointed at the ground when it goes into failsafe mode, it usually will end up back in kit form. In the case of radio controlled heavy machinery, the failsafe settings must be more carfully chosen and programmed. Is power cut off? Are brakes applied? What are the position control presets? Does the failsafe mode depend on the most recent mode of the machine?

I'm assuming that the users of such equipment will have enough sense to employ PCM. They've shown no such sense so far. A construction company in Texas has petitioned the FCC to employ 75 MHz frequencies to operate heavy machinery. These frequencies are attractive because they are license-free and the only currently authorized users are radio control car and boat operators. In the spirit of commercial exploitation of the airwaves, the construction company wants to SHARE those frequencies! That's right - your kid's toy Baja racer may be on the same frequency as a 10 ton bulldozer.

On a related topic, the proposed "person-finder" transmitters, used to locate missing persons, will operate on the same frequencies (72 MHz) as model aircraft. Again, the obvious advantages for those selling such devices are that the frequencies are license-free and the current users are not employing them to make money and so lack political clout. As mentioned by Mr. Horvitz, current FCC policy is to encourage any and all commercial use of the airwaves, without regard to safety or the interests of current users.

Currently, frequency control for model aircraft occurs at club fields and is strictly enforced in accordance with AMA (Academy of Model Aeronautics) regulations. Such control will be moot if the frequencies are shared by "person-finder" transmitters. This is in addition to the previously mentioned (RISKS ?.?) potential for abuse of such devices by employers and the government. The AMA is petitioning the FCC to block frequency sharing.

Caveat: this note was written by a radio control flyer who is a member of the AMA.

Marco C. Barbarisi (AMA # 204356), Naval Coastal Systems Center, Panama City, Florida 32407

Disclaimer: The opinions expressed above are my own and do not necessarily reflect those of the Government, my employer, or the AMA.

## New Yorker Article (book serialization?) on radiation risks

<minow@thundr.enet.dec.com>
18 Jun 89 10:03

Risks Digest readers might find an article series in the current New Yorker interesting. Written by Paul Brodeur, the three-part series is titled "The Hazards of Electromagnetic Fields." The first part, published in the June 12 issue, dealt with power-line magnetic fields and fields generated by high-voltage transmission lines. These are low-level effects that manifest themselves in long-term changes in cancer (primarily childhood) rates.

The current (June 19) issue is concerned primarily with pulsed-microwave fields, especially those from the PAVE PAWS distant early warning radar installations.

The last installment isn't out yet.

One frightening aspect of the problem is the way "scientists" cook their research to suit the "needs" of their funding agencies. For example, Air Force researchers measured the \*average\* emission of PAVE PAWS, which is a multi-megawatt \*pulsed\* beam, rather than its instantaneous intensity.

Martin Minow minow%thundr.dec@decwrl.dec.com

The above does not represent the position of Digital Equipment Corporation.



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 8: Issue 83

Tuesday 20 June 1989

## Contents

Pacemakers, radios

**Walter Roberson** 

'Traffic monitoring system used for spying'

Walter Roberson

I am not a number... (unique postal codes)

Walter Roberson

Medical history-on-a-card?; Another ATM Risks

Edward A. Ranzenbach

Re: Microcomputers in the operating theatre

**Donald Lindsay** 

Keith Emanuel

Hartford Civic Center roof crash

**Peter Desnoyers** 

Re: Risks of missiles

Jan Wolitzky

**Gary Chapman** 

**Bob Ayers** 

Info on RISKS (comp.risks)

#### pacemakers, radios

<Walter\_Roberson@CARLETON.CA> Mon, 19 Jun 89 23:11:58 EST

A small article in The Ottawa Citizen, Fri. June 16, 1989, pg A18:

"Stereo speaker risk to heart device

BOSTON (Reuter) -- Doctors in Chicago have some advice for people whose hearts carry an electronic device for shocking the heart into its proper rhythm -- Don't hug a stereo speaker.

Speakers apparently contain a magnet strong enough to deactivate an automatic implantable cardioverter-defibrillator. The device, usually given to people who have recovered from a heart attack, delivers a jolt to the heart when it begins

beating too rapidly to pump blood."

Walter Roberson

## 'Traffic monitoring system used for spying'

<Walter\_Roberson@CARLETON.CA>
Mon, 19 Jun 89 23:18:09 EST

NEW YORK (AFP) -- Chinese authorities are using a British surveillance system, developed to monitor road traffic, to spy on Chinese citizens and foreigners in the streets of Beijing, Time said in its latest edition.

The weekly news magazine said the so-called SCOOT system had been purchased partially with development aid.

Time also reported that the Beijing State Security Bureau had used the system to document charges against Associated Press reporter John Pomfret, who, the magazine added, was expelled last week after he was filmed meeting with a source in his car outside a hotel in Beijing.

Because the SCOOT system can be used to film at night, it allowed authorities to film fighting outside Tiananmen Square during an army crackdown on pro-reform demonstrations in which western intelligence sources said about 3,000 people died.

Chinese authorities said 100 civilians were killed and about 1,000 others wounded.

The authorities edited the film to show only sequences of aggressive demonstrators attacking peaceful police, Time said.

The sequences were shown on state television, which identified the protestors as counter-revolutionaries.

SCOOT also allowed authorities to pick out individual faces in the crowd. These were also shown on television with a telephone number requesting help from watches in identifying those who participated in the demonstrations. [From The Ottawa Citizen, Mon. June 19, 1989, pg A6]

[Please note: I'm not interested in discussing the politics of the situation in China. I have submitted this article based on the technological -> social implications ONLY. -- WDR]

Walter Roberson < Walter\_Roberson@Carleton.CA>

[Also noted by Mike Olson <mao@postgres.Berkeley.EDU>.]

#### I am not a number... (unique postal codes)

<Walter\_Roberson@CARLETON.CA>
Mon, 19 Jun 89 22:42:37 EST

A few weeks ago, the Canadian post office admitted to a secret "modernization" office they have established. The high-tech research division of the post office. One of the projects they were said to be working on was changing the postal codes from its current 3 letters + 3 numbers, to a 10 "digit" system (unclear whether it'd be pure numeric or not.) I was a little concerned about that at the time: Statistics Canada releases some non-trivial information (eg,

the Canadian census) \*broken down by postal code\*. (As an aside, I've never been too comfortable with that. They do take care that each grouping includes at least 5 people -- but it isn't too hard to extract an individual's data from that, if you know something about the individual.) If StatsCan continued the practice of releasing such information by postal codes, then establishing extremely accurate postal codes is sure to make individual cases much easier to deduce. (And remember, its not only a crime to give incorrect data to the census people: its also a crime to refuse to answer the questions...)

Anyhow, having many other things to occupy my mind, I haven't been thinking about the 10-digit scheme much. None-the-less, I did happen to notice the following, buried in an article about which firm was being favoured to provide some new sorting machines for the post office:

The new equipment will incorperate many features tested by Canada Post in the Paradigm Project, a high-tech research program started about two years ago.

The program, kept secret until last month when it was reported on by the Canadian Press, is being used to test a new 10-digit postal code system Canada Post hopes to introduce within the next few years.

The system is so precise that all addresses in the country, and possibly all individuals, will be assigned individual codes."

[The Ottawa Citizen, Mon. June 19, 1989, pg A4]

After I thought about it for a few seconds, I realized this is a -real-possibility! Canada has about 25 million people, so an 8 digit scheme would be enough to number them all individually (our social insurance numbers are 9 digits, including the check digit). A 10-digit number, then, has more than enough capacity to identify individual people in Canada!

You can have unpublished phone numbers, but will they allow you to have unpublished postal codes? (And if so, will you have to pay extra fo that?)

Oh yes: although this story has a Canadian flavour, note that 10 digits would be enough to encompass all of North America. After-all, phone numbers within North America are only 10 digits, and they haven't run out of phone numbers yet (though they will soon have to expand the area code scheme, which currently only allows the second digit to be a 0 or a 1.)

Walter Roberson < Walter\_Roberson@Carleton.CA>

#### Medical history-on-a-card?; Another ATM Risks

<Ranzenbach@DOCKMASTER.NCSC.MIL> Tue, 20 Jun 89 12:53 EDT

In 1982, CII Honeywell Bull, France, unveiled the "CP-8" smart card. This card does indeed contain a tiny microprocessor and, I believe, 4K of memory. This was envisioned to have uses as an electronic payment card. For example, I would go to a compatible Automated Teller Machine (ATM) and transfer funds from my account to the card. I could then shop with the card at stores with CP-8 compatible readers and use the funds on the card to pay for my purchases. The major difference between this strategy and the Electronic Funds Transfers (EFT)

that we see today is that the CP-8 was deemed as valuable as cash. The repository of account information was the card itself.

Now some may say that EFTs are subject to per-transaction authorization over a network. I know however that my bank does not have a network connection but actually contracts to a larger bank for EFT services. Thus, there is no direct check of my account for authorization. Instead, my bank authorizes a maximum of \$200.00 per 24 hours per customer. The contracted bank simply ensures that I do not exceed that authorization.

An advantage of the CP-8 was its audit trail. All transactions made against the card are audited by the processor and the user can take the card to any CP-8 ATM and receive a printout that shows the date, time, location (machine ID) and amount of the last N transactions. Kind of like having your statement in your wallet.

There were plans in Sweden to implement a scheme for the rationing of liquor purchases from state run liquor stores using the cards but I'm not sure this came to fruition. I'm not sure if this card has found any real uses or if it has been upgraded (4K of memory?).

I saw a couple of risks here. The card is money in my pocket. Although I might not feel confident about walking around the streets of New York with several hundered dollars cash I might be lulled into a false sense of security and think nothing of transfering several hundred dollars to the card. Thus if the card was lost, stolen, or damaged it was the same as having my wallet full of money stolen. In addition to the standard means of damaging the card, we found that significant impact to the surface could damage the cards ability to process or store information (we hit it with a hammer, not very subtle but it showed a weakness).

On a separate but related issue, I found that the password standard for the Cirrus, Star and New York Cash Exchange (NYCE) ATM networks is a four digit password.

I was impressed by the BayBanks ATM network when it first came into being because it offered me a maximum eight (letter) digit password thus giving me 10\*\*8 possible values. During use of my ATM card I noticed that the screen would always flicker as soon as I entered the fourth letter in my password. I decided to "play" a little and noticed that only the first four letters of my password were required to be entered (and thus were included in the validation of my authorization). Thus, there are only 10\*\*4 possible passwords. Cirrus advertizes access to 20,000 ATMs nationwide. Interesting to note that there are twice as many ATMs as possible passwords to protect my account from being misused on them. Maybe someone should send them a copy of the NCSC Password Management Guideline, CSC-STD-002-85...

Edward A. Ranzenbach, Gemini Computers Inc. All standard disclaimers apply.

Re: Microcomputers in the operating theatre

<Donald.Lindsay@MATHOM.GANDALF.CS.CMU.EDU>

Tue, 20 Jun 1989 13:30-EDT

In RISKS-8.82, Ken Howard says:

>Martyn addresses the obvious risk from the hardware/software reliability >point of view here. The other not so obvious risk is that a BBC micro >is not certified for use in an environment containing explosive gasses >such as are used in anesthesia ....

Actually, it's even worse. Operating theatres contain numerous devices, which shouldn't interfere with each other, but do. (An EEG in such a place can often detect brainwaves in lime jello.) There are also standards for electrical leakage - since the patient tends to be a common ground to numerous circuits.

Hospitals also use equipment differently from other places. Suppliers learned years ago that equipment with a flat top will wind up at the bottom of a stack, for example. A flat top will also attract bags, bottles and bowls of fluid, which will get spilled.

I'd also worry about the lack of professional design review. For example, what happens to the patient if there's a power glitch? How about reasonableness checks on dosage? How aware will the operator be of the computer's actions? How quickly could he stop it (emergency off)? My experience with beginning programmers hardly inspires confidence in an MD's first effort.

Don

## ★ Re: Microcomputers in the operating theatre (Thomas, RISKS-8.79)

<Emanuel.henr@Xerox.COM> 20 Jun 89 07:13 EDT

There is more than just performance here. In an operating room the anaesthetist is responsible for his own actions. He bares the consequences of his judgements as a responsible professional.

In the case of a microcomputer malfunction who is responsible? Is it the manufacturer? The programmer? Perhaps the technician who maintains the equipment? Further, Electronics devices have recognized mean times to failure. Does this mean that we are installing a device in a life critical situation that we know will have a failure down the road? Would we certify a doctor who we knew would fail?

Lastly, the state of the art in software expert systems is still a long way from being able to deal with the subtle differences between patients or subtle changes in a patient's condition during an operation. It is for that reason that the doctor is indispensible (no pun).

Keith Emanuel, Xerox Corp.

## Hartford Civic Center roof crash (Desnoyers, RISKS-8.81)

Peter Desnoyers <desnoyer@apple.com> Tue, 20 Jun 1989 10:24:34 PDT In <u>RISKS Digest 8.81</u> Richard S. D'Ippolito writes: (in reference to the Hartford Civic Center roof crash of January '78)

[joint was modelled incorrectly as having no eccentricity, when simulation was re-run correctly the roof did not hold.]

>Quite simply, the problem here was: The structure analyzed was not the >structure built.

This may have been only one aspect of a more wide-spread disregard for safety in the construction of the first Civic Center roof. It was widely reported in the local papers afterwards that there had been only one part-time weld inspector during construction - he was a high school math teacher and evidently only worked on Saturdays or something like that. [disclaimer - this is from memory and may not be completely accurate.]

In other words, if they had cared about safety, they might have been more likely to catch errors in the simulation.

Peter Desnoyers, Apple ATG

(408) 974-4469

#### ✓ Re: Risks of missiles

Jan Wolitzky <wolit@cbnewsm.ATT.COM>
20 Jun 89 18:32:28 GMT

- > ... At this
- > point it is gliding until it releases its warheads. The missile has no
- > mechanism for sensing where it is and aiming the warheads accordingly it is
- > just told, BEFORE LAUNCH, "point here, release a warhead, point there, release
- > a warhead, etc." The point is that all errors in the launch are cumulative and
- > no mechanisms exist to correct them.

This is incorrect. There certainly is an inertial guidance system aboard all versions of the Minuteman missile (only IIs and IIIs are currently active). And while is it true that the solid-fuel boosters on such missiles are not throttleable per se, any point up to the missile's maximum range can be targeted by changing the ballistic trajectory. Besides, there \_are\_ various thrust termination mechanisms available for solid rockets (blowing off the nozzle, venting the combustion chamber, etc.), though I am not aware which, if any, are used on the various Minuteman stages.

Even after burnout of the last stage, the warheads of the Minuteman III still do not follow a purely ballistic trajectory. This missile carries three \_independently\_targetable\_ re-entry vehicles, attached to a maneuverable "bus." The bus is powered, and changes its trajectory before releasing each of its warheads. I believe the maximum separation between targets of warheads on a single missile is classified information.

Finally, more recent warheads (tested on the MX missile) are themselves

maneuverable during re-entry, for evading ABMs. There is evidence that the D5 warhead being developed for the Trident II missile will use satellite navigation signals from the Navstar Global Positioning System (GPS) for terminal guidance. (The Pershing II warhead, incidentally used Terrain-Contour Matching (Tercom) radar for terminal guidance.) These mechanisms could remove much of the uncertainty involved in firing missile over previously unflown trajectories.

Please forgive my lengthy response, especially since I am uncertain what this discussion is doing in comp.risks in the first place.

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

## Re: Risks of missiles

Gary Chapman <chapman@csli.Stanford.EDU> Mon, 19 Jun 89 15:43:09 PDT

I don't want to drag out a discussion of ICBMs, which probably belongs in ARMS-D, but just to offer an addendum, or a slight correction, to Steven Den Beste's recent posting (RISKS 8.82, Risks of Missiles). He said that all tests of Minuteman missiles have been conducted in flights from Vandenberg to Kwajalein atoll. Actually there have been four tests of Minuteman missiles launched from silos, and all four of them failed.

-- Gary Chapman
Executive Director, Computer Professionals for Social Responsibility

#### ★ Re: Descriptions of Minuteman Missiles

Bob Ayers <ayers@src.dec.com> Mon, 19 Jun 89 17:21:50 PDT

I am not an expert on missile systems, but even from the little knowledge tht I have, I do not believe the statements of denbeste@BBN.COM about the Minuteman system. He writes (in risks 8.82) "The missile has no mechanism for sensing where it is and aiming the warheads accordingly ... all errors in the launch are cumulative and no mechanisms exist to correct them."

I suggest that, while the Minuteman has no mechanism that actually \_looks\_ to see where it is, it \_does\_ have positional feedback in the form of intertial mavigation subsystems. So it is \_not\_ travelling in a "dead reckoning" mode as the end of the above quotation asserts.

And I find the bald statement that the Van Allen belt and the different "g" field in northern regions damage missle targeting, with no supporting remarks whatsoever, to be .. um .. curious. I don't know, and I doubt that he knows, either -- though I would be very surprised to learn that the U.S. military doesn't understand the Earth's gravitational field and its effects on bodies in icbm trajectories.



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 8: Issue 84

# Wednesday 21 June 1989

## **Contents**

The risks of global editing

Martyn Thomas / Richard Tobin / Nick Radcliffe

- Re: I am not a number -- already in the US
  - Tom Comeau
- Re: I am not a number -- more in Canada Vince Manis)
- Re: Computer electrocutes chess player ... W. Scott Meeks
  - **Brendan McKay**
- Gigatext Translation Services Inc. scandal **Bhota San**
- Info on RISKS (comp.risks)

## The risks of global editing

Martyn Thomas <mct@praxis.UUCP> Wed, 21 Jun 89 14:23:59 BST

From today's Guardian (UK national newspaper), Wednesday 21st June

"Correction

Because of the startling simplicity of computer programme logic, the Labour Party's successful candidate in the London South West seat of the European elections was printed on Monday as Ms A J Turnoutack, rather than Ms A J Pollack. On Tuesday, her name was again spelt incorrectly.

The computer programme which run [sic] to massage the results into printed form changed each occurrence of the work Poll, into Turnout."

(Spotted by Simon Seely)

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK.

[Also reported by Richard Tobin <richard@aiai.edinburgh.ac.uk> (who added that the Guardian has been noted for its misprints since long before computers), and by Nick Radcliffe <njr@etive.edinburgh.ac.uk>.

I suppose Turnoutyanna would have seen the good even in that one. But in a fault-tolerant illumination system there would have been an unfortunate ambiguity between Poll the Lights and Turnout the Lights. PGN]

#### Re: I am not a number - already in the US

"Chairman, Von Neumann Catastrophe Relief Fund" <TCOMEAU@STSYSC.UUCP> Wed, 21 Jun 89 10:29:44 EDT

In <u>RISKS DIGEST 8.83</u>, Walter Roberson discussed a possible Canadian move to ten digit postal codes. While most people in the US don't use more than the first five digits, the US Postal Service (USPS) already uses a 9 digit ZIP+FOUR code.

Like Canada, the census people give out info based on ZIP code, and it is a crime not to give accurate information. So I trotted down to the local post office, and sure enough, my address is a unique nine digit code. There are only four units in my building, and only nine people, so a person with census info based on nine digits and just a little more (like, I'm the only married male in my building) can find out anything the census bureau know about me.

We just got a note last week (delivered by the USPS to OCCUPANT) that the 1990 census is coming, with assurances that our responses to the census would be kept strictly confidential. In light of this RISKS discussion, I'll have to take that claim up with both the Census Bureau and my elected representatives.

tc> Tom Comeau, Sr Systems Manager, Space Telescope Science Institute, 3700 San Martin Drive, Baltimore, MD 21218 (301) 338-4749 (AT&T)

Disclaimer: My opinions are my own, not even my wife agrees with me.

## I am not a number... (unique postal codes)

Vince Manis <manis@grads.cs.ubc.ca> Wed. 21 Jun 89 08:19:12 PDT

Walter Roberson describes the proposal to create a 10-character postal code, and mentions that it seems to generate a too-high degree of discrimination. (The current postal code, of which V6T 1W5 is an example, does an excellent job: the first character corresponds to the province, and the first three to the Forward Sortation Area (FSA), or sorting station; the full code corresponds to less than a single carrier's route. Further, the mixture of letters and digits substantially lowers the error rate, because transposition errors, the most common among fast typists, result in invalid codes.)

There is, however, a RISK which is entirely separate from the assault on privacy which a 10-character code would inevitably produce. It is necessary to realise that Canada Post's service is legendarily atrocious (though not perhaps as bad as that of the Italian Post Office, which once shredded 40 tonnes of

mail which had taken so long to sort that it wasn't worth delivering). The introduction of postal codes in 1974 was supposed to speed service. In fact, service has deteriorated. (It is quite common for a first-class letter to take a week to be delivered to another address in the same sortation area.)

Labour relations are also atrocious at Canada Post. There are at present several tens of thousands of in-process grievances; the leadership of the main postal union is highly radicalised; and management has made it very clear that it is not interested in improving the situation.

When the original code was introduced, the postal workers opposed it, fearing a loss of jobs. They stamped 'Boycott the code' on letters, and protested strenuously. Management didn't do anything in particular to smooth the transition.

I can see the introduction of a longer code as an excuse to create further confrontation, thus excusing the awful service. So long as long delivery delays can be blamed on `lazy workers', whereas the Corporation is using the latest technology to expedite things, nobody really has to do anything specific to fix the serious management/labour problems at Canada Post.

Ain't technology wonderful?

Vincent Manis, The Invisible City of Kitezh, Department of Computer Science, University of British Columbia, Vancouver, BC, Canada V6T 1W5 (604) 228-2394

#### Re: Computer electrocutes chess player who beat it!

W. Scott Meeks <wscott@flab.flab.fujitsu.junet> Wed, 21 Jun 89 11:12:59 JST

It occurred to me that there may be a very plausible explanation for this story--there was indeed a murder comitted, but not by the computer. It seems to me that the programmer, research scientist, whoever, who programmed this super computer may have been embarrased (perhaps fatally in political terms) by the fact that his system was being beaten my a mere human. To get revenge, he reprograms the computer, possibly modifying the chess board as well to make the fatal short circuit, so that it electrocutes the chess master the next time the computer loses. This may even turn out as an added bonus for the researcher -- the computer may not be able to beat a chess master, but it is intelligent enough to stand trial. Once again, the computer gets all the blame.

W. Scott Meeks, Bellcore, Morristown, NJ 07960-1910

## ★ Re: Computer electrocutes chess player who beat it! (RISKS 8.75)

Brendan McKay <bdm@anucsd.oz.au>
21 Jun 89 10:18:35 EST (Wed)

[Dave Horsfall doubts that 12 volts can cause substantial electric shock.]

On the contrary. About a year ago I drove my car into a creek and got stuck. I tried to disconnect the battery but found it quite impossible to hold onto the positive terminal without insulation; the shock was sufficient to make my arm flail around uncontrollably. I was standing in about one meter of water, and the car was turned off. (Of course, I should have disconnected the negative terminal instead, but nobody's perfect.)

PS. Haven't people been electrocuted in swimming pools by remarkably small voltages? I defer to someone who knows the details.

Brendan McKay. bdm@anucsd.oz.au

## Gigatext Translation Services Inc. scandal

Bhota San <VOGTWARR@UREGINA1.BITNET> Wed, 21 June 1989 1:35:43 CST

For some of you, this will be the third time you will have been exposed to this article. I apologize for this. The first time was intentional, but only the subscribers on Bitnet got it. The second time was because of an anomaly in the file transfer mechanism, unintentional. This time it is so that the non-Bitnet subscribers can read it and so that I can finish the story of the whole ludicrous affair. Also, one of the respondents sent me the complete references for the books I consulted to form an opinion of this misbegotten venture. If you wish you can skip the repeated section of this posting and go straight to his upgraded bibliography and the story's denouement by typing FIND BIBLIOGRAPHY or some other search command to move your editor to that point in my account. But that is several lines ahead. The repeated introductory section begins here:

/ Tues, 13 June 1989

The provincial government of Sask., Canada is now embroiled in a scandal over its involvement with an AI language translation company owned by Guy Montpetit of Montreal, a shady dealer currently defending himself against a \$39-million lawsuit for not paying back loans. Deputy Premier Eric Berntson had discussed with Montpetit the possibility of its investing \$125 million in a computer chip foundry, the details of which would have been overseen by Montpetit.

But the government has already invested \$4 million in Montpetit's GigaText, a company established to translate by computer Saskatchewan's statutes into French. A couple of years ago, a local Francophone created a sensation when he took to the Canadian Supreme Court his case that his constitutional rights were being infringed when he had to go to court on a traffic ticket that was made out to him in English, not French. The Court decided in his favour. After trying to quash the decision by a decree of its own, the government swore it would save millions of dollars by getting someone to create AI software to translate its laws, rather than by hiring bilingual humans to translate them "the old way". The government accepted Montpetit's offer to do the job and payed him the \$4 million to rent a sizable office complex, hire administrative personnel and a few programmers supposedly bilingual and conversant in Lisp and Prolog. It is alleged that the government also bought him a luxury home, payed his plane fare to "conventions", and let him use a Mercedes to get to his Re-

gina appointments. It took a long time for expert criticism of the presumptions of this venture to reach the public, including the NDP opposition which is now raking the incumbent PC's over the coals for it. But Berntson confidently predicts the computerized translator will be unveiled in full working condition on June 17.

That's four days from now. It will be interesting to see how it turns out. From everything I have read, Artificial Intelligence language translation is still a long, long way from being practicable, and indeed may be impossible. The world will stand up and take notice of what has been accomplished in Regina Sask. on June 17, but I wonder if it will be for the reasons Berntson intended.

I based my assessment of this case on readings from a book called "Turing's Man" by J. David Bolter. (See references below.) On a different subject is a book called "The Fifth Generation Fallacy", by J. Marshall Unger. The author, a professor of East Asian languages at the University of Hawaii, Honolulu states that the REAL reasons the Japanese are in such a rush to invent this new hard- & software has little to do with fifth generation machines that imitate human neural networks & thought processes to speak to the user in his own tongue [sic]. It is their desperation to find a means to speedily process, store & distinguish the thirty odd thousand characters of their Kanji script. These characters are difficult to represent digitally or on a screen: It takes a 24 X 24 grid (576 bits) to store a good image of them. To keypunch, input them will be yet harder: Business memos are still written out in hand. And it will seriously test the software running at extremely high speed to tell them apart, aside from the grammatical difficulties involved. In short, the professor believes the Kanji character system puts an immovable limit on what any computer technology can do for their quest for data-handling speed and efficiency. The question is then: Do the dubious advantages of increased productivity obtained by high-tech mean more to the Japanese than love of their culture and the elegance of their 1000-year-old Kanji script?

#### **BIBLIOGRAPHY**:

Bolter, J. David, 1951- <UBOLT@TUCC.BITNET>

Turing's man: western culture in the computer age / by J. David Bolter. -

Chapel Hill: University of North Carolina Press, c1984.

xii, 264 p.: ill.; 24 cm.

Unger, J. Marshall.

The fifth generation fallacy: why Japan is betting its future on artificial intelligence / J. Marshall Unger. - New York: Oxford University Press, 1987.

x, 230 p.: ill.; 22 cm.

DENOUEMENT

Tues, 20 June 1989

Well, a week has passed and now I can report what happened on June 17, the day Sask. deputy premier Eric Berntson promised to show us the computerized French-English translator, working as planned. For it is certain he had something planned, and it came as a surprise to everyone.

Mr. Berntson did not have a scrap of translated laws to show us that day. But he did succeed in showing us the NDP opposition was guilty of having wasted more of the tax-payers' money when it was in power over something like this than the incumbent PC's have over GigaText. As he said, in 1981 "the New

Democratic Party...invested \$5 million -- the equivalent of \$8 million today -- in an outfit called Nabu...from central Canada [and] not one job, not one ounce of technology moved to Saskatchewan. The whole investment was written off and these technological wizards over there blew \$5 million!"

Nabu developed informational or educational software programs for home entertainment. Embarrassed by this telling repartee, the NDP critics fell into sullen silence. (The Leader-Post, June 17 p A4)

Yet the NDP's venture, an investment in what we would probably call an "expert system", from a purely technical perspective had a greater chance of succeeding than did the PC's venture into the field of Al language translation, a goal that continues to elude the most accomplished researchers in this area. (See "Turing's Man" in the above bibliography.) Herbert Clute (ABC Translation) agrees with ex-director of legislation translation in neighbouring Manitoba, Greg Yost's opinion that machine translation of its statutes was "too primitive to be of any use." He said weather reports are the only material that can be translated flawlessly: "If the vocabulary is straightforward and limited, machine translation would be a great saving in time, but we all know laws aren't straightforward."

Manitoba gave the bulk of its translation contract to "Traduction Universelle", a Montreal-based company in contact with plenty of people who were competent to translate the language in specific areas of legislation. In four years the bulk of the translation, 4000 pages, was translated by the Dec. 1988 deadline for public laws and regulations. (The Leader-Post, June 19, 1989 p A4)

Saskatchewan, in contrast, since July 1988 has funnelled \$5.25 million into the GigaText Translation system, so far without success. PC politicians have had to face accusations of wasting the money on perks for Montpetit and to take off his hands obsolete computers from his own company. The 20 GigaMos computers that GigaText bought for its Regina research centre cost the government \$152 000 each. Their cost climbed from \$1,5 million to \$2,9 million as they passed through the hands of firms owned either by Montpetit or his close associates before being purchased by GigaText. Montpetit's U.S. company "Systems" manufactured them. (The Leader-Post, June 16, 1989 p A4)

Incidentally, Berntson acknowledged meeting am associate of Montpetit named Dr. Alex Voshchenkov. He considers Voshchenkov to be one of the world's leading high-tech scientists and declared, "if I can find a way that is reasonable to get Dr. Voshchenkov and his technology into Saskatchewan I would like to do it." I am unfamiliar with Dr. Voshchenkov and his achievements, but with that June 17 deadline passed, the provincial government will need all the help it can get! (The Leader-Post, June 17, 1989 p A4)

The RCMP has been investigating Montpetit to determine how GigaText spent SEDCO's first \$4 million. There are allegations Montpetit spent it on overpriced computers, personal debts, payments to those who helped arrange the government financing, and jet travel, like a weekend flight taken by Montpetit and a female companion to San Francisco at a cost to GigaText of \$15 000.

In exchange for its \$4 million, the government got 25% ownership in the company. In exchange for his unproven technology, Montpetit and his partner were given 75% control and sole responsability for signing cheques. This continued, even after he was named in a \$39 million lawsuit last October, until he was eased out in March. A new \$1,25 million SEDCO loan was provided to keep the company alive, but the June 17 deadline was set for it to prove it could do its job. That day has come and gone. You'd think that would be the end of it, but the project has been given a stay of execution. Berntson said that because June 17 was a Saturday, the deadline is being extended to some time this week. If at

the last moment, it miraculously succeeds, I will faithfully report the details to the list. But if you don't hear from me again, you can assume it will have been the big flop everyone expects. After all, there is an old Latin maxim that fits very well here: "DE MORTUIS NIHIL NISI BONUM."



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 8: Issue 85

## Wednesday 28 June 1989

#### Contents

Air Force satellite positioning system cracked

**Dave Curry** 

Loose wire caused Clapham train crash

Jon Jacky

London firms reportedly offer amnesty to ``hacker thieves"

Ken Berkun via Jon Jacky

Re: Microcomputers in the operating theater

Jon Jacky

**Diomidis Spinellis** 

Don't celebrate big tax refund too quickly

**David Sherman** 

Reading meters and gauges by robot in nuclear power plants

Robert Cooper

Info on RISKS (comp.risks)

## Air Force satellite positioning system cracked

<davy@riacs.edu> Wed, 21 Jun 89 22:43:43 -0700

Taken from the San Jose Mercury News, 6/21/89 (from the Kansas City Star):

Teen hacker hits satellite guide system

A 14-year-old Prarie Village, Kan., boy, using a small home computer, cracked an Air Force satellite-positioning system and browsed the confidential files of at least 200 companies, officials say.

The teen-ager, a computer hacker since the age of 8, apparently did not damage the computer systems he easily entered during the past six months. He hoped to use his know-how to persuade the companies to hire him as a computer security consultant, police said.

At least two military investigators and representatives of several companies, including Hewlett-Packard Co. of Palo Alto, showed up at a meeting this month in Johnson County to try to find out how he did it.

Dialing unauthorized long-distance access codes, authorities say, the teenager linked his Apple computer with systems throughout the country. He specialized in cracking the H-P 3000, a Hewlett-Packard minicomputer widely used by businesses and the federal government.

At one point, authorities say, he gained access to an unclassified Air Force computer system.

[Other than in the first paragraph, there's no more mention of what, if anything, the kid did to the satellite positioning system. The comment that he was hoping to be hired seems intriguing to me; I wonder if there's now a wave of "interview by cracking" starting up? --Dave]

### Loose wire caused Clapham train crash

<JON.JACKY@GAFFER.RAD.WASHINGTON.EDU>
23 Jun 1989 11:59:16 EST

Here are excerpts from IEEE INSTITUTE, May 1989, p. 4:

"British train accidents signal systemic problems" by Fred Guterl and Erin E. Murphy

... Sloppy installation caused (a) recent fatal train accident..., according to Britrail, the state-run railway system ...

On Dec. 12 at the busy Clapham junction in south London, ... one commuter train plowed into the back of another, killing 35 and injuring almost 100. ... In that accident, according to British Rail, the evidence found so far points to an installation error made a few years ago, when British Rail replaced the older electromagnetic switches in its signalling system at Clapham. ... during this process an equipment room wire from an old switch was not properly removed and came into contact with the new electromagnetic signaling system.

The signaling system regulates the movement of a train from one section of track to another. ... The presence of current indicates both that the next section of track is unoccupied and what the next signal's setting is. ... At Clapham, the loose wire directly operated the signal, overriding the checks in the system and causing the signal to turn green. The signaling system was thought to be fail-safe because a short circuit would simply cause a red light. ...

The worker who has taken responsibility for leaving the wire loose testified in the inquiry that on that day he had worked more than 12 hours with only a 5-minute break ...

- Jon Jacky, University of Washington

✓ London firms reportedly offer amnesty to "hacker thieves"

<JON.JACKY@GAFFER.RAD.WASHINGTON.EDU [Originally from Ken Berkum}> 23 Jun 1989 12:09:06 EST

[This comes to me from a friend who lives in Hong Kong. - Jon Jacky]

From: kenberkun%hgovc.DEC@decwrl.dec.com (Ken Berkun)

Reported in the June 12, 1989 South China Morning Post, apparently reprinted from the London Times, retyped by me, without permission.

Headline: "Worried firms pay hush money to 'hacker' thieves"

By Richard Caseby

Firms in the City of London are buying the silence of hackers who break into their computers and steal millions of pounds.

At least six London firms have signed agreements with criminals, offering them amnesties if they return part of the money. The firms fear that if they prosecute they will lose business when customers learn that their computer security is flawed.

In several of the case the losses exceeded 1 million pounds but only a tenth of the total was returned.

The Computer Industry Research Unit (CIRU) which uncovered the deals and which is advising the Department of Trade and Industry in data security, believes the practice of offering amnesties is widespread.

"Companies who feel vulnerable are running scared by agreeing to these immoral deals. Their selfishness is storing up serious problems for everyone else," said Peter Nancarrow, a senior consultant.

Police have warned that deals struck with criminals could possibly lead to an employer being prosecuted for perverting the course of justice.

Detective Inspector John Austin, of Scotland Yard's computer fraud squad, said: "Employers could find themselves in very deep water by such strenuous efforts to protect the credibility of their image."

Legal experts say the firms are mking use of section five of the Criminal Law Act 1967 which allows them to keep silent on crimes and privately agree on compensation. However, an employer becomes a witness to the offence by taking evidence from a criminal when the deal is drawn up.

Hackers steal by electronically transferring funds or by programming a computer to round off all transactions by a tiny amount and diverting the money to a separate account.

In one case, an assistant programmer at a merchant bank diverted 8

million pounds to a Swiss bank account and then gave back 7 million in return for a non-disclosure agreement portecting him against prosecution.

Such thefts have spread alarm throughout the City, with consultants offering to penetrate the computer networks of banks and finance houses to pinpoint loopholes before a hacker does.

The biggest contracts cost up to 50,000 pounds and can involve a four month investigation in which every weakness is explored.

Detectives have found that computer security at many City institutions is riddled with loopholes. A City of London police operation, codenamed Comcheck, revealed wide spread weaknesses. Firms were asked to track the number of unauthorized logons over Easter bank holiday.

Some companies unable to tell whether hackers had penetrated their network, while others lacked any security defences.

In addition to theft, companies are vulnerable to blackmail. Hackers can threaton to sabotage computers by inserting "viruses" and "logic bombs" - rogue programs which can paralyse a system.

This type of threat has prompted the offer of a new insurance policy underwritten by Lloyd's which specifically covers viruses and other computer catastrophes.

## ★ Re: Microcomputers in the operating theater

<JON.JACKY@GAFFER.RAD.WASHINGTON.EDU>
23 Jun 1989 13:01:44 EST

There are computer-controlled drug infusion devices on the market; they are definitely not hobbyist items. IVAC Corporation of San Diego has made several presentations at technical meetings recently about a new product of theirs called the Titrator (registered trademark) Sodium Nitroprusside Closed Loop Module, which began development in 1981 and was finally approved by the FDA in December, 1987.

The FDA began regulating medical device software in 1987. IVAC believes its device was the first to be reviewed by the FDA under the new regulations. Two papers about their experience appear in PROCEEDINGS ON THE ENGINEERING OF COMPUTER-BASED MEDICAL SYSTEMS, June 8-10, 1988, Minneapolis, Minnesota, published by the IEEE Computer Society: ``The travail involved in getting FDA approval --- an overview of what it took to get FDA approval of a medical device with computer technology (a recent experience)'' by Albert Paul, pps. 28--29, and ``Failsafe design of closed loop systems'' by Alvis J. Somerville, pps. 23--27.

- Jonathan Jacky, University of Washington

## Re: Microcomputers in the operating theatre

Diomidis Spinellis <diomidis@ecrcvax.UUCP> Thu, 22 Jun 89 10:37:41 +0200

Keith Emanuel, brings up the question of responsibility in the case of a microcomputer malfunction. I remember that National Semiconductor data sheets used to have a warning to the effect that the component described should not be used on any life critical application without prior written permission from the company. They defined a life critical application as one whose malfunction or failure to operate could cause human deaths or injury. I have not seen such a warning in data sheets of other manufacturers, so it is probable that this problem has a precise legal answer.

Diomidis Spinellis, European Computer Industry Research Centre (ECRC).

## Don't celebrate big tax refund too quickly

David Sherman <dave@lsuc.on.ca> Tue, 27 Jun 89 14:48:07 EDT

Toronto Star, June 27, 1989, page B3:

About 6,000 people across Canada have received extra-large refunds after filing their 1988 income tax returns, and must return the excess. Clyde King, spokesman for Revenue Canada's Toronto office, said yesterday the people affected pay quarterly tax instalments. These taxpayers, the self-employed and some retired people, must pay the instalments because they're not subject to withholding at source on the bulk of their income. King said that in some cases Revenue Canada's computer in Ottawa added the first-quarter 1989 tax instalment to the 1988 refund due, resulting in the excessive refund.

Though about 70,000 people were affected, the error was caught in all but about 6,000 cases before the cheques were sent. In many cases, taxpayers have contacted Revenue Canada and sent back the excess. Eventually the others will be sent letters of explanation and asked for the return of the money."

[Comment 1: I like the "Revenue Canada's computer added" part. People don't create bugs, computers create bugs.]

[Comment 2: one hopes that as well as fixing the bug, they have correctly fixed the accounts of people whose 1989 instalments may not have been credited properly as of the date due...]

David Sherman, Tax Lawyer, Toronto

★ Reading meters and gauges by robot in nuclear power plants.

Robert Cooper <rcbc@honir.cs.cornell.edu> 28 Jun 89 21:16:31 GMT

The June issue of IEEE Computer Magazine contains an article on a robot vision system which reads analogue and digital meters, lights, and determines valve, slider and switch positions:

"A Vision System for Robotic Inspection and Manipulation" M. Trivedi, C. Chen, and S. Marapane Computer Magazine, June 1989, p. 91.

<The authors envisage a system such as their's being used to inspect and monitor nuclear power plants:

"Although most of our findings relate to a broad class of industrial automation tasks, the specific operational environment we considered was a nuclear power plant, where robotic inspection offers the potential for reduced radiation exposure to personnel and lower plant operating costs."

However the authors, who are funded by the Department of Energy, do not discuss the risks of relying on such technology in critical applications such as nuclear power plants. The ONLY allusion to any possible misgivings people might have to this technology is:

"These tasks need not be performed totally autonomously; a human observer can interpret images acquired by staionary cameras or those mounted on robots."

There would appear to be several, more robust, more easily validated alternatives to this technology. In particular, using a robot vision system to read an LCD display seems to be a rather expensive and error prone implementation of a wire!

I feel that anyone proposing a software system for use in critical applications must discuss the risks involved. And an article in a broad readership professional magazine such a Computer would be the ideal place.

-- Robert Cooper (rcbc@cs.cornell.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 8: Issue 86

# Thursday 29 June 1989

#### Contents

SPADOC Modernization Effort

**Chris McDonald** 

Are are nuclear weapons useable? How can one test this?

Dennis L. Mumaugh

NASA tests video system that may lead to windowless cockpits

Karl Lehenbauer

Air Force to upgrade missile launch command computers Jon Jacky

Missile launch -- upgrades degrade?

**Clifford Johnson** 

Strategic weapon software development practices

Stan Shebs via Jon Jacky

Rotting Landsat data Jonathan Patrick Leech

Info on RISKS (comp.risks)

### SPADOC Modernization Effort

Chris McDonald ASQNC-TWS-RA 678-4176 <cmcdonal@wsmr-emh10.army.mil> Mon, 26 Jun 89 11:59:53 MDT

The General Accounting Office (GAO) has issued a report, 20 Apr 89, entitled "Management and Technical Problems Delay Operation Center Acquisition" (GAO/IMTEC-89-18). The 50+page report discusses the Air Force Space Defense Operations Center modernization effort at Cheyenne Mountain.

The following is from the Executive Summary:

"The SPADOC program has been marked by management problems, unrealized expectations, and program delays. The Air Force has invested over \$235 million in a system that is now more than 4 years behind schedule and far from meeting its required operational capability.

At the root of SPADOC's technical problems is the Air Force's attempt to achieve controlled mode security. Software development tasks designed to achieve this form of multilevel security are time-consuming, technically demanding, and still undergoing much research and development. In SPADOC's case, functions such as notifying national decision makers that a satellite is under attack take as much as four times longer to complete than required."

Interested parties can call 202-275-6241 to obtain a free copy. In the interest of fairness the DoD/Air Force response is included within the report.

#### Are are nuclear weapons useable? How can one test this?

<cuuxb!dlm@att.att.com>
Thu, 22 Jun 89 20:17 CDT

My uncle is a conspiracy and doomsday person and several friends have worked in the "business". They have given me an education. My own experiences in a military organization have confirmed their observations:

The major problem is that only a couple of times has our nuclear arsenal been tested under field conditions (to the public's knowledgee). Even then it has not really been under battle conditions.

The major problem is that today's military rarely have surprise tests.

Operational Readiness Tests(ORT) would have to simulate a true war. This would include a lot of collateral information and details, lack of warning, and other items. Anything less than firing random rockets would not be a real test.

Also there are cross checks to make sure other missiles are being fired.

The current worry is that 1). The missile crews might freeze or panic. 2). The missile would explode on the pad or fail to fire. 3). It wouldn't get airborne - blast through the silo lid. 4). It would cartwheel in the air or explode (as one recent test did). 5). It wouldn't hit the target.

The problem is testing this because any commander who has word of an inspection or a ORT will prep his equipment and men. The phemonena of the perfect troop of military is well known to inspecting generals and chiefs of state as well as the GIs who are told to prepare for a "surprise inspection".

The risk? How do you test a doomsday machine. Can any system be tested for "ultimate load" or "emergency conditions".

=Dennis L. Mumaugh
Lisle, IL ...!{att,|||-crg,attunix}!cuuxb!dlm OR dlm@cuuxb.att.com

#### NASA tests video system that may lead to windowless cockpits

Karl Lehenbauer <karl@cs.utexas.edu> 22 Jun 89 23:16:33 CDT (Thu) NASA and McDonnel Douglas are testing a helmet-mounted, visual approach and landing system that could have applications for future aircraft without cockpit windows, according to the June 19, 1989 issue of Aviation Week and Space Technology (pages 126 and 127). The system uses two fixed-position monochrome video cameras mounted in the aircraft's nose. Video and graphics processing is performed, and digitized pictures are relayed to the helmet display.

According to Mark S. Rolwes, principal investigator for McDonnell Douglas, the use of a fixed sensor suite offers advantages such as high reliability (because there are no moving parts) and redundancy.

A magnetic tracking device is used to measure the pilot's head movements. Based on where the pilot is "looking", a 30 by 40 degree field of view is selected, processed and displayed on the helmet's eyepieces.

There is a 17-millisecond delay in getting an image from the cameras to the eyepieces. Rolwes said the delay is imperceptible and that it doesn't affect pilot performance.

All four pilots in the tests were able to successfully land NASA's Boeing 737 Transport Systems Research Vehicle aircraft using the landing system, coming within 500 feet of a specified target after making several practice approaches. A second pilot was present to set up the approach and be ready to take over and fly the aircraft visually if there was a problem with the landing system.

I won't belabor RISKS readers by enumerating a bunch of the obvious potential problems with such a system. Suffice to say that the possibility of crashing an airplane because of a failure in the video system, coupled with the inability to look out the window (because the plane doesn't have one) is terrifying.

The article specifically mentions future hypersonic flight vehicles as aircraft that may not have, or be able to have, conventional cockpit windows. Also, it says that the system could have applications in current military aircraft in which crew eye protection during combat is important.

For commercial aircraft, the system would supposedly be useful for obviating window area restrictions and for providing night vision capabilities. Although this touches on a whole kettle of risks that have been undergoing periodic discussion in this forum (risks from too much going on in the cockpit, etc), I think that such a system, if well-designed, could help to reduce the possibility of an accident, as long as a manual backup system (a window) was retained.

#### Air Force to upgrade missile launch command computers

<JON.JACKY@GAFFER.RAD.WASHINGTON.EDU>
23 Jun 1989 11:19:12 EST

Here are excerpts from FEDERAL COMPUTER WEEK, May 8 1989, p. 10:

"Air Force to Upgrade Missile Control Systems" by Bob Brewin

The Air Force plans to upgrade the computer and communications systems that run the launch control centers of the US long-range missile arsenal. The \$507 million project will streamline the authentication of war order messages as well as missile retargeting and launch authorization, according to the Air Force.

Under the Rapid Execution and Combat Targeting (REACT) contract, the Air Force plans to automate for the first time the processing of emergency war order messages by the two-man intercontinental ballistic-missile launch control center crews. Part of the job includes improvements in the 1960s-vintage weapons system control computers that manage the launch and retargeting of all missiles in a wing.

Although the REACT system features an electronic interface between the war order message processing function and weapon control systems, an Air Force official said, "The nuclear assuredness aspects of the system will remain the same. Man will remain in the loop." ...

Bruce Blair, a former launch control center (LCC) officer who studies nuclear command and control systems for the Brookings Institution, said that while the REACT program ``will reduce human judgment at [the LCC level] by some factor," its impact will be minimal ``because most of the human judgments are made at the NORAD or National Command Authority level." ...

LCC crews receive war order messages through three digital communications channels: very low frequency radio, the Air Force Satellite Communications System and the SAC digital information network. According to Brooking's Blair, the crews must then take these messages and manually authenticate them with secured code books. The computerized message processor would handle these tasks, including sorting through duplicate messages, automatically. "We're going to let the machine sort through all the messages and then present the information on the screen to the crew member," (Col. Michael) Mazzaro (a REACT program manager) said. After authenticity checks are completed, the processed messages, together with retargeting information, are passed via an electronic interface to the weapons system control element. Mazzaro said that although the system has been automated, "this is not the stuff of the 'War Games' scenario. Man is in the loop the entire way. He makes the decisions"...

The planned modifications ``will permit LCC's to stay on alert beyond the turn of this century," (the Air Force) said. [The article explained the new system would be used with Minuteman, MX, and possibly future Midgetman and rail garrison MX missiles].

REACT consists of two different but related programs managed by the Electronic Systems Division (ESD) and the Ballistics Systems Division (BSD) of the Air Force Systems Command. ESD will manage development of the higher-authority communications and rapid message processing element for which GTE government systems was awarded ... \$33.7 million. ... BSD awarded Ford Aerospace ... \$71.3 million for development of the Weapon System Control Element, which includes rapid retargeting systems, voice communications, control consoles and displays, the weapons system processor and modifications to existing LCC trainers. . BSD officials ... estimated the total value (of the upgrade effort) at \$507 million

- ... Ford based its architecture on the Raytheon MilVax. BSD officials have said they have not determined whether to use existing code or new code for the weapons system control element.
- Jon Jacky, University of Washington.

#### Missile launch -- upgrades degrade?

"Clifford Johnson" <GA.CJJ@Forsythe.Stanford.EDU> Fri, 23 Jun 89 14:29:16 PDT

Jon's posting re SAC's REACT missile launch ugrade is just another relentless turn of the hair-trigger screw. Another turn is reported in this month's Air Force Magazine, which is all about AF electronics. An article reports:

The Ground Wave Emergency Network (GWEN) [is] a multi-stationed net of LF radio towers and receivers... Electronic Systems Division (ESD), working with RCA, has nearly completed installing an initial, 56-node "thin-line" segment for flashing [one-way] emergency messages [launch orders] to Strategic Air Command units.

With glasnost and perestroika afoot, and the JCS visiting the U.S.S.R., must we reduce SAC's standing response time from over to under a minute? Is anyone seriously weighing the concomitant risks?

[By the way,] for those who don't know, on May 1 this year I filed a lawsuit against the Strategic Air Command's chain of command for launching Minuteman and MX missiles, including the launch crews, alleging that their standing orders, to launch the missiles immediately upon receipt of cryptologically valid launch orders, are inherently reckless and dangerous. In particular, I allege with particularity the risk of mistaken computer prompts causing the accidental launch of nuclear missiles. The suit was endorsed by the board of Computer Professionals for Social Responsibility.

In a motion to dismiss based on the pleadings, which presumes that all facts alleged be taken as true, here is Commander In Chief General Chain's (minion-attorney's) key argument:

The allegation of "high risk" may affect the amount of speculation but only marginally, and it does not move the allegation into the realm of injury in fact. At most, plaintiff makes the general assertion that some government officials may act in a manner contrary to law.

## Strategic weapon software development practices

<JON.JACKY@GAFFER.RAD.WASHINGTON.EDU>
29 Jun 1989 11:00:41 EST

Several recent postings in this digest have speculated about the accuracy/quality of strategic weapons guidance systems. Apropos of that, I offer the following excerpts from an article by Stan Shebs, about working on cruise missile guidance, that appeared in the CPSR/Seattle Newsletter, June 1988:

from "My Life in a Megadeath Corporation" by Stan Shebs

Upon graduation from Texas A&M in 1981, I accepted an offer from Boeing Aerospace in Seattle ... I was re-assigned to work on the cruise missile.

I went off to Seattle (Kent actually) and started work. This involved fingerprinting (a surprise) and the long long form to fill out (for a clearance, even though I never did anything classified). Next thing was to jump in on the work, which was to help finish up and deliver "mission planning" software - a giant mass of undocumented Fortran intended to run on IBM mainframes at SAC headquarters in Nebraska. My first task was to finish testing the FORMVO module, which had to do with figuring out which VOs (Vertical Obstructions - like trees and telephone poles) were likely to be in the path of the missile as it flew along.

If this is confusing, well, it was to me too. After about a month, I went to the official orientation and indoctrination, which lasted about two days. Boeing was building the Air-Launched Cruise Missile (ALCM), essentially a robot airplane about 6 meters long and 1/2 in diameter, powered by a jet engine of just the right size for a go-cart, and carrying a 400-kiloton fusion bomb. The idea was that B-52 bombers would fly up to the edge of the USSR, launch the ALCMs, and fly away again. The missiles would then fly about 2000 km or so, low to the ground and beneath radars all the way, to detonate at some target. ... Now the onboard software was basically done; where I came in was to help with the software that figures out if an intended route was actually doable. The onboard computer has only a very limited capacity, so you need a lot of "mission planning" software to decide where to turn, how high to fly, when to look at the ground to see if you're on course, and so forth. Another piece of software then makes up the cute little cassette tapes that the bomber crew loads into the missile before launching it. It's tricky, because how tight a turn the missile can make depends on how much fuel it's used already, it could run into telephone wires if it's flying too low at the wrong moment, the little maps that it uses for navigation mustn't be too far apart, and so forth.

The difficulty of all this apparently didn't occur to anybody until after the missile was working, so the mission planning software got hacked out in a real hurry, the people that did it departed for greener pastures, and then the rest of us were picking up the pieces and trying to turn all this into a reasonably reliable 40,000 lines of Fortran. The day-to-day work was like regular software stuff; debugging a program that took map data from tapes and put them into VSAM files, writing the "Program Design" for an already-written program (is that stupid or what), figuring out how to compute the intersection of two polygons in space. We supposedly had a "model" software engineering methodology; what I remember most clearly is that half the work was done on one flavor of IBM OS, and the other half done on a different flavor, and file transfer between the two was tricky and time-consuming.

The fragility of something like the cruise missile and its software is something I've spent a lot of time wondering about, and don't really have any idea. The nuclear safety aspect seemed pretty good - there was at least some effort to get accurate estimates of the chance of going off at the wrong time (was 1 in 2^64 chance, I think). Navigation is considerably more problematic. Like most missiles, ALCM relies on inertial navigation, but the error accumulation over 2000 km is immense, and you had to be sure to have navigation maps spaced so there would be a reasonably good chance they would be found. ("3-sigma" was the standard - position assumed to be a normal distribution.) Now that I think about it, the 3-sigma test (98% chance) would have to be multiplied for each map, and there might be 10-20 of them, meaning as much as 40% of missiles might not make it through all the maps... Calculations on a sphere were a perennial problem - there was a standard joke that the safest place in the world during a nuclear exchange was the North Pole, because the lat/long singularity makes it impossible to target, and the worst place was 0 lat, 0 long, because the software would divide by 0 or overflow or something while passing over the North Pole and reset to all Os... The precision and formality of the software was very low, but it was exhaustively tested over and over and over again. I suppose the greatest risk of failure derives from things that weren't anticipated during testing, such as a Siberian snowdrift changing the topography on a navigation map...

(Regarding) statistics on software quality, the closest thing we had was maybe a count of problem reports (hundreds, but each report ranged from one-liners to one-monthers in terms of effort required). ... the humongous requirements document that was our bible for how the program was supposed to work (was) alternately entertaining and horrifying. Nothing classified, we had the odd situation that the \*data\* was classified, but the \*program\* wasn't even rated "confidential"! (Theory was that the Russians were supposed to get a copy, which would set them back ten years...:-) ) ...

#### Rotting Landsat data

Jonathan Patrick Leech, Apple Integrated Systems <leech@Apple.COM> 29 Jun 89 22:14:04 GMT

From the June 16 \_Science\_ article "Early Data: Losing Our Memory?":

"Allen Watkins, director of the USGS center in Sioux Falls, SD, where Landsat tapes are kept, says, "90% of the data collected before 1979 are now inaccessible." The reason: the data tapes were recorded on old Xerox computers which can no longer be operated. In addition, the satellite location and timing data were recorded on a kind of video tape deck that no longer exists. Tape renewal is another problem that looms in the future. Magnetic images "bleed" through the layers as time passes, and tapes must be recopied at least once every 10 years to make them usable. Watkins says the task is already formidable, and wonders what will happen when the Earth Observing System begins sending back the equivalent of an entire Landsat archive every 2 weeks."



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 8: Issue 87

# Thursday 29 June 1989

#### **Contents**

"Student plan marred by computer mistake"

**Matthew Wall** 

Immigration Chief Proposes National Computer Screen

Christopher T. Jewell

Big Brother is Hallucinating

Elizabeth D Zwicky

Study finds "pedal misapplication" to blame for Audi surges Jon Jacky

Computer Crime and Social Risks

Pete McVay

Reducing risks of cost overruns/project failures

Pete Lucas

Re: New Yorker Article on radiation risks

**David Chase** 

Computerized Translations

Will Martin

Info on RISKS (comp.risks)

#### "Student plan marred by computer mistake"

Matthew Wall <WALL%BRANDEIS.BITNET@mitvma.mit.edu> Fri, 23 Jun 89 09:45 EDT

The complete text of an article in the Boston Globe, 6/23/89. pp. 13,83 (reproduced without permission)

Student plan marred by computer mistake

by Diego Ribadeneira, Globe Staff

In a major glitch in the new Boston school student assignment plan, a computer tape containing the names of nearly 900 students entering kindergarten this fall was lost, leaving parents unsure if their children will be able to attend their preferred schools.

The snafu, discovered earlier this week, also hurts the credibility of the plan, which some critics had said was being implemented too rapidly.

Some students who have already received their assignments for next year may not have gotten their top choices had the tape with the 900 applicants been properly processed, school officials said.

Superintendent Laval S. Wilson said the department has not yet determined how it will remedy the problem. He said it may conduct the assignment process for kindergarten students all over again. The error occurred, according to school officials, because the lost tape had been used to test the accuracy of a program developed to assign schools to students under the new plan. The tape was not returned to be used in the computer run to assign students to schools.

"Inadvertently this tape was not merged with the other tapes...," said Catherine Ellison, senior officer for implementation for the Boston School Department. The lost tape contained the names of 887 children, the majority of whom will be entering kindergarten.

Since the mistake was discovered, school officials have manually been able to match 344 of the children on the misplaced tape with one of their school choices.

Under the plan, called controlled choice, the city is divided into three geographic zones. Parents were asked to list five choices for schools within their zone. The plan will being this fall for students entering kindergarten, first grade and sixth grade. All remaining grades would fall under the new plan in the fall of 1990.

School officials had advised parents affected by the new plan to submit their applications by May 18, the first deadline for choosing a school, to have a better chance of getting their top choices.

The officials acknowledged yesterday that the remaining 543 students on the misplaced tape may not get one of their preferred schools, partly as a result of the mistake.

"We will be looking at the remaining applicants to determine how well we can honor the requests," Ellison said. "We will do as much as we can with the best interests of the parents in mind. I won't sit here and promise something I cannot deliver. We hope to attempt to honor one of the parents choices."

Kathy Satut listed the New Agassiz School in Jamaica Plain as her first choice.

"I called up Wednesday and that's when they told me they had lost the tape." Satut said. "I couldn't believe they had done that. Now I don't know what's going to happen. Am I going to be penalized for their mistake? What was the point of trying to get the application in on time. I think they should all be fired. I'm very, very upset."

School officials said they are trying to insure that the percentage of students from the misplaced tape who get their first choice will be about the same as that for the students assigned schools from the first computer run. They said they hope to complete assignments for kindergarten students by the weekend.

News of the error angered some school observers who said it comes at a time when various reforms are being undertaken in an effort to lure new students to the system.

"It's pretty outrageous," said Paula Georges, executive director of the Citywide Education Coalition. "It undermines the credibility of the plan."

[End of Text]

[The most obvious implication of this incident is the importance of having a

backup. And why oh why weren't they using a \*copy\* of the data to do their testing?!? The article merely hints at some intriguing characteristics of the Boston Schools' DP department.

What disturbs me about this is that the plan is an important step in the troubled recent history of the Boston schools towards equitable access to various resources within the schools, by allowing parents to make an informed choice for their child as to which school to attend. This ``snafu'' has created the perception of arbitrary school assignments. Further, I suspect the complicated nature of giving the maximum number of students one of five top choices involves so many permutations that computer processing is essential to proceeding with the plan; as the article reveals, the ``credibility'' of both the plan, and most likely the role of computer processing, has now been called into serious doubt.]

### Immigration Chief Proposes National Computer Screen

<chrisj@cup.portal.com>
Fri, 23-Jun-89 15:14:14 PDT

Friday June 23 N Y Times, p. A10: By Roberto Suro, special to the NYT

LA JOLLA, CA, June 22 -- The Commissioner of Immigration and Naturalization, Alan C. Nelson, today proposed a nationwide computer system to verify the identities of all job applicants in order to halt the widspread use of fraudulent documents by illegal aliens seeking jobs.

Mr Nelson also suggested standardized identity cards for immigrants so as to get fuller compliance with a 1986 law prohibiting employment of illegal aliens.

Creating a national identity card and other ways of checking legal status or identity have been repeatedly suggested in Congress as tools in fighting unlawful immigration, but have also been consistently rejected as potential infringements on civil liberties.

[15 column-inches deleted]

The national computerized database on everybody is one bad idea that simply refuses to stay dead, no matter how many times we drive a stake through its heart---if the INS ("Search warrants? We don't need no stinking search warrants!") didn't resurrect it, the drug czar or the FBI would. "Eternal vigilance ...". On the other hand, it appears to me that most informed citizens by now understand the risks involved: computer professionals no longer have to fight this battle alone.

The identity-card stuff I suppose belongs in talk.politics.misc: I won't go into it here.

Chris chrisj@cup.portal.com sun!cup.portal.com!chrisj (Christopher T. Jewell) chrisj@netcom.uucp apple!netcom!chrisj

#### ✓ Big Brother is Hallucinating

Elizabeth D Zwicky <zwicky@cis.ohio-state.edu> Thu, 22 Jun 89 10:49:32 EDT

I've seen a fair number of articles in the press lately warning people about how sophisticated advertisers are getting in keeping databases and targetting particular groups. I wonder if any of their authors has been getting the targetted junk mail I have.

Oh sure, I get junk mail targetted towards Mazda owners, because I bought one recently - but I get equally large amounts of junk mail for Camry owners, that being the car I sold when I bought the Mazda. Some of my junk mail is targetted to childless single mid-twenties women; then again, the same week brought me mail that confidently announced that the coupons inside were specifically targetted towards "growing families like mine, with young children" and mail that confidently announced that I had now reached "an interesting age" (from context, they meant I was over 40) and my children were all grown! Not to mention the advertisements that begin "Men like you..."

I understand why they think I own a Toyota; I have a vague concept that my growing family was a guess based on the date of my marriage certificate, which definitely made its way into databases. I am at a loss to explain how anybody became certain that I was over 40, or that I was male. I also wonder why (and how) people manage to keep such careful track of car purchases but not sales, marriage but not divorce... My mother, who has been dead nearly 5 years, has reached retirement age in the databases that are preserving her memory for the advertisers of America.

All in all, I don't think I'll worry about Big Brother watching me in order to sell things to me.

Elizabeth Zwicky

#### Study finds "pedal misapplication" to blame for Audi surges

<JON.JACKY@GAFFER.RAD.WASHINGTON.EDU>
23 Jun 1989 11:44:31 EST

Here are excerpts from IEEE INSTITUTE, July 1989, p. 8:

``Study finds `pedal misapplication' to blame for Audi surges' by Karen Fitzgerald

The Audi 5000 has largely been vindicated in claims over the last four years of sudden, out-of-control acceleration, but a U.S. National Highway Traffic Safety Administration (NHTSA) study released in March also cautioned that pedal design and minor engine acceleration may have caused drivers to apply their foot to the accelerator instead of the brake. ...

The study, "An Examination of Sudden Acceleration," explored ... electromagnetic and radio frequency interference and malfunctions in cruise control, electronic idle-speed control systems, computer-controlled fuel

injection systems, transmissions, and brakes. The investigators could find no mechanism --- besides actuation of the gas pedal --- that would open the throttle sufficiently to accelerate any of the cars studied at full power.

However, there was evidence of minor surges of about three-tenths of the Earth's gravity for 2 seconds caused by electronic faults in the idle stabilizer systems of the Audi 5000 ... the surge could startle a driver enough to accidentally push the accelerator instead of the brake, the study found ... Moreover, the travel of the pedals and their height off the floor make it possible for engine torque to overtake brake torque when the pedals are applied simultaneously ... [ more about this, including a graph indicating unusually problematic placement of pedals in the Audi ].

The NHTSA took pains to call the problem "pedal misapplication" rather than "driver error," as Audi first characterized the problem. ... "Driver error may imply carelessness or wilfulness in failing to operate a car properly," said an NHTSA press release announcing the study. "...(sudden acceleration) could happen to even the most attentive driver who inadvertantly selects the wrong pedal and continues to do so unwittingly."

- Jon Jacky, University of Washington

#### Computer Crime and Social Risks

Pete McVay, TAY2-2/F14, 227-3598 <pmcvay%comcad.DEC@src.dec.com> Thu, 29 Jun 89 05:42:19 PDT

Social Comment: Are computer criminals, and is computer crime, treated differently than other crimes?

RISKS DIGEST 8.85 (28 June) carried two separate stories on hackers, their motives, and the results of their "activities".

In one case, a teenager managed to crack the code of an Air Force satellite and was able to read confidential information of at least 200 companies: "He hoped to use his know-how to persuade the companies to hire him as a computer security consultant, police said."

The second article reported that "Firms in the City of London are buying the silence of hackers who break into their computers and steal millions of pounds."

I have personal knowledge of similar incidents of both types:

- o One hacker, very notorious to telecommunications security people, was finally apprehended, and some of the on-line evidence in his personal accounts showed that he had planned to use his cracking expertise to get a job in the computer industry.
- o I have never heard of any payoffs, such as are reported in the second article--but it is well known among security and legal consultants that companies will often drop a hacker case because of fear of publicity.

In fact, some of the security experts have been "turned to the dark side of hacking": frustrated by their own company's refusal to crack down on lawbreaking, they have become phone phreaks and crackers themselves.

There is a persistent piece of folklore that criminals in nonviolent crimes are often hired as consultants by the industries or governments they victimized. I can't remember the source exactly--but I remember a report a few years back from some U.S. Government enforcement agency that such things are very rare; in fact, the incidents of such hiring are all well documented as special cases. But in computer crime it appears to be a norm that criminal activity will go unpunished, and might even be rewarded.

If the social controls aren't in step with legal controls, then the best laws and enforcement systems are worthless. Companies and governments publicly decry cracking of all types: they often state that the public should be educated that breaking into telecommunications circuits (computers or otherwise) is a crime. Yet these same companies/agencies refuse to enforce existing laws--and some crackers have been hired as consultants or paid off.

I don't pretend to have a good answer to this problem. Perhaps the "social" definition of computer crime needs to be changed; maybe we're dealing with a new and different kind of social behavior and the rules must be examined. Personally I favor more enforcement of existing laws, perhaps backed up with a new law that would not allow companies/agencies to drop charges once an arrest was made (a frequent occurrence). However, something needs to be done: as long as this social/legal dichotomy exists, no progress (or protection) exists for the socially responsible hacker and computer user.



<"Pete Lucas, NERC Swindon UK."> Wed, 21 Jun 89 16:02:32 BST

<PJML%ibma.nerc-wallingford.ac.uk@NSFnet-Relay.AC.UK> Subject: Reducing risks of cost overruns/project failures

Much of recent discussions have been relating to products which have no guarantee of working (missile systems). From a purely technical point of view this reflects badly on the procurement process. Would you buy a dishwasher/TV/microwave/automobile/aircraft if you couldn't see a working model (and what's more, try it for yourself) first? Wouldn't you expect it to come with a warranty against faulty design or workmanship? Surely when DoD pays billions of dollars for a weapons system, the taxpayer is entitled to expect that the supplier will provide a meaningful warranty, and that any failures will be pursued in a rigorous and thorough manner (i.e. through the courts).. There appear, to my way of thinking, two areas of conflict::

1) In a large project, involving many thousands of man-years effort, it is (almost) impossible to, at some point, admit that there's been a mistake made previously - this leads to embarassment and red faces all round. Hence, previous mistakes, misunderstandings etc. get fossilised into the system at an early stage and are never undone. There is no

easy way of avoiding these sorts of problems when the coverup may only come to light when the article/project is completed (by which time it's too late to do anything about it as the money has all been spent.....)

Solutions - well i am a confirmed minimalist when it comes to these areas, 'Keep-it-simple-Stupid' (KISS) technology can avoid a number of possible failure modes (and save money too - why buy one very sophisticated system when you can have more less complex (and hence probably more reliable!) ones? The `if it isn't there it won't go wrong' argument against complexity is a powerful one - minimising component count by eliminating unnecessarily complex functionality means that the thing will be more likely to work when you need it to. It also keeps the human-count down (and as we all know, people are the most error-prone and irrational parts of any system!). Remember that the number of failure modes increases dramatically with the number of points of failure.

If a large company intended to sell me some device, i would insist on a test-drive, on MY chosen patch (so the supplier couldn't present his device under the most satisfactory conditions) and if the supplier couldn't deliver, then he sure wouldn't get the cash! It's amazing how withholding payment will concentrate the minds of people. 'Cost-plus' contracts are a mistake too, as you don't know what the final cost will be. The classic example here is the British 'Nimrod' project - a plan to produce a radar-plane functionally equivalent to AWACS - after ten years and nearly a billion pounds of funding, it was scrapped (and AWACS bought...).

If I had been the UK government, someone somewhere wouldn't be in business any more.... After all, we all pay TAXES (don't we?) and so it's OUR money and i think we should EXPECT things to WORK when the time comes..!!!

Pete Lucas

[This contribution covers ground that will be familiar to many RISKS readers, and is somewhat OVERsimplified, but nevertheless makes some good points. PGN]

#### Re: New Yorker Article on radiation risks (RISKS 8.82)

<chase@orc.olivetti.com>
Tue, 27 Jun 89 13:37:01 -0700

The third part in the series is on radiation and alleged health problems associated with VDTs. It is worth reading -- it was sufficiently detailed to give a former "they should have accounted for job stress" skeptic (me) reason to wonder.

Several points taken from the series (as recalled and interpreted by me):

- consider \*magnetic\* fields, not just \*electrical\* fields (easier to shield against electrical fields)
- 2) The strength and range of magnetic fields depends on geometry and current -- the low-voltage distribution lines in your back yard may emit just as strong a magnetic field as the high voltage lines through some farmer's fields. Though magnetic fields fall off rapidly with distance, fields from large "coils" extend farther than fields from small "coils" (that is, household appliances are much smaller than power distribution systems, and thus their magnetic fields are of different shape and size).
- 3) consider not just VDT operators, but also people sitting around the VDT operators (there's the horizontal deflection coil which emits a 10s of KHz sawtooth, and the vertical deflection which emits a 50-100 Hz sawtooth. The strong portions of those fields may not extend directly to the front of the VDT).
- 4) be careful, in general, when people quote "average" figures at you; the repetitive peak power is also an important figure. The frequency spectrum is also interesting -- harmonic effects have been observed.
- 5) There have been studies (on magnetic fields in general).

  Effects have been observed, both statistically (leukemia stats) and experimentally (abnormal development of fetal chickens and mice). The mechanism, if any, is unknown.

\*Interactions with the ambient (i.e., earth's) magnetic field have been observed\* -- this affects repeatability of experiments if not controlled for.

David

#### Computerized Translations

Will Martin <wmartin@ST-LOUIS-EMH2.ARMY.MIL> Thu, 22 Jun 89 15:54:04 CDT

Thanks to Bhota San for the posting on the Canadian computer-translation item. This reminded me of something I had just seen in a recent paper, and which struck me as odd at the time. However, since I didn't know what the curent state-of-the-art was in computerized translation, I didn't realize at the time that this precis of a US Army Request for Proposal represented some really pie-in-the-sky hopes for a fantastic level of AI in automated translation! Here is the item, from the "CBD Watch" column [CBD = Commerce Business Daily] on page 24 in the June 5, 1989 issue of Federal Computer Week:

Army. Software for language translation. Software must be capable of translating from English to German, Spanish, French, Italian, Japanese, Korean, Chinese and Portugese. It must provide idiomatic, verbatim translation of such documents as military specs, international legal agreements, correspondence, reports, studies and military briefings on doctrine, combat developments, training and materials. It must be MS-DOS compatible and capable of translating military terms and syntax. Contact Barbara Smith, TRADOC Contracting Activity, Building 1748, Fort Eustis, VA 23604-5538, (804) 878-4053. \*\*\*End of item\*\*\*

Hmmm... So these people expect this to run on a PC, too... (note the "MS-DOS" reference...) "TRADOC" is the Training and Doctrine Command, by the way. I can see why they would want to be able to translate stuff for the training of allied personnel. However, based on the info in the previous posting, it sure seems unlikely they are going to get what they want! Also, the RISKS implications of this are rather stupendous. To expect software to translate both military jargon, circumlocution, and tortured governmentese prose, and at the same time handle the diplomatic nuances of "international legal agreements" is a bit much, I think... Most multi-lingual humans would have difficulty doing that.

Will Martin



Search RISKS using swish-e

Report problems with the web pages to the maintainer