Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Index to Volume 7

Thursday 22 December 1988

- Issue 1 (1 Jun 88)
  - RISKS of Evolution and Evolution of RISKS (PGN)
  - Re: Risks of automatic test acknowledgement (Paul Traina)
  - Computing Down Under (Willis H. Ware)
  - Computer Tampering Case to go to Trial (Joe Morris)
  - Software can destroy hardware (Willis Johnson and John B. Nagle via danno)
  - Cash on the Nail, by Daedalus (Brian Randell, Jacob Oestergaard Baekke)
  - Re: Down in the Dumps (Stan R.Z., Mark W. Eichin, Dan Klein, Dan Franklin)
- Issue 2 (2 Jun 88)
  - Happenstance and $70 Million (Patrick A. Townson)
  - Re: Optimisers too tacit, perhaps? (Tim McDaniel)
  - Re: Optimisers; Telecommunications Redundancy (Michael Wagner)
  - Major security hole in some sun systems (Pete Cottrell and Steve Miller and Jim Purtilo and Chris Torek)
- Issue 3 (3 Jun 88)
  - OTA Report: Science, Technology, and the First Amendment (Jan Wolitzky)
  - Disasters and computer facilities (Rodney Hoffman)
  - Running as root; Hinsdale redundacy; Daedelus (David Herron)
  - Optimizing PL/I (Bard Bloom)
  - Re: Auckland cable cars (Richard A. O'Keefe)
  - My experience with metal balloons (David J. Edgerton)
  - Halon (Romain Kang)
  - Virus collection (Robert Slade)
- Issue 4 (6 Jun 88)
  - Review article on privacy/civil liberties risks in CACM (Jon Jacky)
  - RISKS of wrong numbers and tigers (Steve Nuchia)
  - Academic Assignment of Viruses (Bill Murray)
  - Peter J. Denning on Terminology (Bill Kinnersley)
  - COMPASS '88 PROGRAM (Frank Houston)
  - Halon agreement and the ozone models (Rob Horn)
- Issue 5 (7 Jun 88)

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

Issue 6 (8 Jun 88)

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

Issue 7 (10 Jun 88)

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

Issue 8 (16 Jun 88)

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

Issue 9 (22 Jun 88)

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

Issue 10 (27 Jun 88)

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

Issue 11 (29 Jun 88)

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

Issue 12 (30 Jun 88)

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

Issue 13 (1 Jul 88)

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

Issue 14 (1 Jul 88)

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

Issue 15 (5 Jul 88)

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

Issue 16 (6 Jul 88)

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

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

Issue 17 (8 Jul 88)

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

Issue 18 (8 Jul 88)

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

Issue 19 (10 Jul 88)

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

Issue 20 (11 Jul 88)

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

Issue 21 (13 Jul 88)

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

Mouse trap (James H. Coombs)
- Threshold probability for declaring a radar blip "hostile" (Mike Wellman, Clifford Johnson)

Issue 22 (14 Jul 88)

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

Issue 23 (16 Jul 88)

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

Issue 24 (18 Jul 88)

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

Issue 25 (20 Jul 88)

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

Issue 26 (24 Jul 88)

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

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

Issue 27 (25 Jul 88)

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

Issue 28 (26 Jul 88)

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

Issue 29 (27 Jul 88)

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

Issue 30 (29 Jul 88)

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

Issue 31 (8 Aug 88)

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

Computer terminals and dermatology (richard welty)
- Computer System Vulnerabilities (Rodney Hoffman)
- Disaster Exposition (Cliff Stoll)

Issue 32 (9 Aug 88)

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

Issue 33 (10 Aug 88)

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

Issue 34 (12 Aug 88)

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

Issue 35 (15 Aug 88)

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

Issue 36 (17 Aug 88)

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

Issue 37 (19 Aug 88)

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

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

Issue 38 (22 Aug 88)

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

Issue 39 (24 Aug 88)

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

Issue 40 (25 Aug 88)

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

Issue 41 (31 Aug 88)

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

Issue 42 (1 Sep 88)

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

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

Issue 43 (2 Sep 88)

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

Issue 44 (5 Sep 88)

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

Issue 45 (7 Sep 88)

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

Issue 46 (7 Sep 88)

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

Issue 47 (8 Sep 88)

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

Issue 48 (9 Sep 88)

- COMPASS 88 (Bev Littlewood)

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

Issue 49 (11 Sep 88)

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

Issue 50 (12 Sep 88)

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

Issue 51 (13 Sep 88)

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

Issue 52 (14 Sep 88)

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

- Issue 53 (15 Sep 88)
  - Hurricane Gilbert (Richard A. Schafer via Matthew P Wiener)
  - Phobos I details (Dave Fiske, Jack Goldberg)
  - Computers and Elections (Lance J. Hoffman)
  - The First "Virus" on Japanese PC (Yoshio Oyanagi)
  - Another one-key mishap (Larry Nathanson)
  - Re: "Single keystroke" (Warren R. Carithers, Paul Dubuc)
  - More computer follies -- how not to design a console (Seth Gordon)
  - GNU Emacs & Security (A.Gaynor via Eliot Lear and Geoff Goodfellow)
  - Complex phones (Dave Fetrow)
  - ISDN/ANI - What one switch vendor told me (Allen L. Chesley)
- Issue 54 (16 Sep 88)
  - CerGro voice mail hacked (John Sheneman)
  - Re: Computer error in vote tallying (Andy Frake)
  - IEEE approval voting (Don Chiasson)
  - Reminder -- ROM is not necessarily nonalterable (Andrew Klossner)
  - Colwich Junction (Mark Brader)
  - Smoke Inhalation on Amtrak's "Crescent" (Mike Trout)
  - Computer assigned hotel rooms (Bruce Wampler)
- Issue 55 (17 Sep 88)
  - The Ethics of Conflict Simulation (Mike Trout)
  - Re: Social content of video games (Tim Wood)
  - Re: Credit Doctors (Dave Robbins)
  - Virus in ROM on commodore 64 (Jurjen N.E. Bos)
  - Re: Destructive remote controls (Henry Spencer, Jurjen N.E. Bos)
  - Another one-key mishap (Russ Nelson)
  - Call for Papers, Invitational Workshop on Data Integrity (Zella Ruthberg)
- Issue 56 (21 Sep 88)
  - Runaway mouse problem in popular commercial WP program (Jon Jacky)
  - Wrapping Britain round the Greenwich meridian (Jack Campin)
  - Crime and (indifferent) Punishment (Glen Matthews)
  - Software Mixup on Soyuz Spacecraft (Karl Lehenbauer)
  - RISKS of (Suspected) Crooks Running Dinosaur-DOS (Fred Baube)
  - Multiple reservations and single bills (Jacob Hugart via Markus Stumptner)
  - Complete info on the Phobos 1 (Kaj Wiik via Ritchey Ruff)
  - `Computer programmer convicted of creating "virus"' (Mike Linnig)
- Issue 57 (24 Sep 88)
  - Faulty locks delay prison opening (Henry Cox)
  - In the future, risks of purchasing handguns (Alan Kaminsky)
  - Olympian RISKS (Henry Cox)
  - [Another Willamette] Sewage Spill Linked to Computer (Nike Horton)
  - Keep backups, risk job (James F. Carter)
  - Computer failure shuts down several thousand telephones (Vince Manis)
  - LA Times photo of humorous credit card maybe not so funny (Michael Coleman)
  - Risks of Cellular Phones? (Chuck Weinstock)
  - Auto Computer Risks (Chuck Weinstock)
  - Volvo's and Electromagnetic Interference (Bill Welch)

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

Issue 58 (26 Sep 88)

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

Issue 59 (29 Sep 88)

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

Issue 60 (3 Oct 88)

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

Issue 61 (5 Oct 88)

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

Issue 62 (7 Oct 88)

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

- Issue 63 (10 Oct 88)
  - Re: Killer terminals (Steve Wilson)
  - Can't Happen and Antilock Braking Systems (Marcus Barrow and Robert Allen, via Mark Brader)
  - ATM's credit check (Amos Shapir)
  - Dive Computers (Terry S. Arnold, Henry Spencer)
  - Emergency Access to Unlisted Telephone Numbers (Dave Wortman)
  - Re: Risks of Cellular Phones (Wes Plouff, Peter Robinson, Walter Doerr)
  - Computers, Copyright Law, and the Honor System (a talk) (Mark Mandel)
- Issue 64 (13 Oct 88)
  - 100 digit primes no longer safe in crypto (Dave Curry)
  - Risks of computer controlled doors (Piet van Oostrum)
  - NSFnet Backbone Shot (Gene Spafford)
  - Intersection of ANI and Voice Mail Risks (Gary McClelland)
  - New Feynman book (Eugene Miya)
  - High `Rev'ing Volvo (Hartel)
  - Stevie Wonder gives an Ear-itating Performance (Marshall Jose, PGN)
  - OMB "Blacklist"? (Hugh Miller)
  - Re: Ethics of Conflict Simulation (Scott Wilde)
- Issue 65 (15 Oct 88)
  - Vendor introduces "safe" Ada subset (Jonathan Jacky)
  - Re: ethics of conflict simulation (Sean Malloy)
  - Re: Assault on Privacy (Ronni Rosenberg)
  - Software warranties and Trade Practices in Australia (B L Coombs annoted by "cbp", via Lee Naish)
  - RISKS of EPROMS (George Sukenick)
- Issue 66 (20 Oct 88)
  - British computer calls Northern Ireland a "Region Unknown" (John Murray)
  - "Brain" virus shows up in Hong Kong (Dave Horsfall)
  - A Credit Card Fraud (Brian Randell)
  - Nausea-inducing propellor (Mike Trout)
  - Re: Ear-itating performance (Jan Wolitzky, Ken Johnson)
- Issue 67 (25 Oct 88)
  - Unplugged Cable Plugs Orlando Traffic (Scot E Wilcoxon)
  - Airbus A320 in service (Henry Spencer)
  - Computer Literacy (Ronni Rosenberg)
  - Belgian PM's email tapped (Rodney Hoffman)
  - Police find hacker...and release him (Henry Cox)
  - Aegis user interface changes planned (Jon Jacky)
  - Programmable Hotel Locks (Allen J. Baum via John Rushby)
  - Nausea-inducing frequencies (David Chase)
  - Risks in Foundations of Numerical Analysis (John Cherniavsky)
  - Takeoff warning systems to be tested (Henry Cox)
- Issue 68 (31 Oct 88)
  - Conspiracy to Defraud (Martyn Thomas)
  - `Runaway' Computer Projects (Rodney Hoffman)
  - Perceived risk (James F. Carter)

"TCA pushes for privacy on corporate networks" (Jerry Leichter)
- Risks in Answering Machines (Andy Glew)
- Ear-itation (Ed Ravin)

Issue 69 (3 Nov 88)

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

Issue 70 (3 Nov 88)

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

Issue 71 (6 Nov 88)

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

Issue 72 (8 Nov 88)

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

Issue 73 (9 Nov 88)

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

Issue 74 (10 Nov 88)

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

Issue 75 (11 Nov 88)

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

Issue 76 (12 Nov 88)

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

Issue 77 (14 Nov 88)

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

Issue 78 (15 Nov 88)

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

Issue 79 (16 Nov 88)

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

The FBI Wants You (if you were virus-ized) (Tom Zmudzinski via Dave Curry)
- Access and authorization (Joe Morris)
- Laws of computer evidence (Barry C. Nelson)
- Call for comments on uniformity legislation for software (Conleth S. O'Connell via Alan Kaminsky)

Issue 80 (18 Nov 88)

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

Issue 81 (21 Nov 88)

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

Issue 82 (23 Nov 88)

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

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

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

Issue 84 (29 Nov 88)

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

Corps of Software Engineers? (Henry Spencer)
- Software Uniformity Legislation (Colin M Thomson)
- Zapping shoplifters in Minnesota (Scot E Wilcoxon)
- (Counter-)corrective control systems (Jeffrey R Kell)

Issue 85 (1 Dec 88)

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

Issue 86 (3 Dec 88)

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

Issue 87 (5 Dec 88)

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

Issue 88 (6 Dec 88)

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

Issue 89 (6 Dec 88)

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

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

Issue 90 (8 Dec 88)

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

Issue 91 (11 Dec 88)

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

Issue 92 (12 Dec 88)

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

Issue 93 (13 Dec 88)

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

Issue 94 (15 Dec 88)

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

Issue 95 (16 Dec 88)

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

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

Issue 96 (20 Dec 88)

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

Issue 97 (21 Dec 88)

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

Issue 98 (22 Dec 88)

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

Report problems with the web pages to the maintainer

THE RISKS DIGEST

Forum On Risks To The Public In Computers And Related Systems

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

Search RISKS using swish-e

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

- Vol 26 Issue 47 (Monday 6 June 2011) <= Latest Issue
- Vol 26 Issue 46 (Saturday 4 June 2011)
- Vol 26 Issue 45 (Tuesday 24 May 2011)

- News about the RISKS web pages
- Subscriptions, contributions and archives

Feeds

RSS 1.0 (full text)

RSS 2.0 (full text)

ATOM (full text)

RDF feed

WAP (latest issue)

Simplified (latest issue)

Smartphone (latest issue)
Under Development!!

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

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

Selectors for locating a particular issue from a volume

Volume number: Volume Issue Number: Issue

Get Specific Issue

Volume Index

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

Index to the RISKS Digest

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

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

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 1

Wednesday 1 June 1988

Contents

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

RISKS of Evolution and Evolution of RISKS

Peter G. Neumann <NEUMANN@csl.sri.com>
Wed 1 June 88 16:45:00 PDT

Welcome to Volume 7! There have been 472 RISKS issues in the past 35 months. However, the number of contributions has been expanding dramatically of late as RISKS goes further out into the internet. (I note the big increase in messages from Australia!) (Countering that somewhat is the appearance of specialized groups, such as VIRUS-L.) To prevent RISKS readers from being totally inundated with the deluge, the proportion of messages emerging from my pipeline has been dwindling somewhat of late -- as I sharpen my interpretation of the above guidelines. (Apologies to those of you who did not get any response at all -- if you feel that your contribution was of

PARTICULARLY BURNING INTEREST and that I might have missed it or not gotten it, please resubmit with a note -- or think about refining it.) By the way, RISKS production will have to slow down a little during June, because of my schedule; so, be patient. Maybe with school recesses, discussion will slow down also. But the world never rests, and we can assume that there will be a few stellar cases of interest to RISKS. PGN

Re: Risks of automatic test acknowledgement (RISKS-6.93)

Paul Traina <comdesign!pst@unix.SRI.COM>
Tue, 31 May 88 11:56:55 PDT

As one of the culprits who found this feature in Erik Fair's *.test message bouncer program, I'd like to mention a couple of ways to protect yourself (by the way, yes, it was an accident).

What is a *.test message bouncer? If a user posts a message to "misc.test" or "alt.test" this bouncer program will mail the posted message back to the user. This is often used by sites to determine if their news feeds are making it out to the backbone (or, as in our case, to gather statistics to determine the best news propigation path).

The symptom is that this one particular (the most popular) message bouncer will send mail to every address on every From: line in the message. This includes From: lines in the message body. Now that this feature has been widely publicised in the "news.admin" newsgroup, the best step is to warn everyone before some net-terrorist decides to cause real havoc.

The message that caused the recent problems on the net had two features which, when combined, resulted in a mess.

(1) the message had 109 From: lines in the body
(2) it was a large ~62k message

What happened? Every site that had the message bouncer installed sent out 109 62k mail messages. Also, many of these mail messages failed because of a bad address. This lead to them to be bounced back to the originating site (the one with the bouncer) to end up in the inbox of the Postmaster. Needless to say, many sites had their spool partitions and usr partitions filled to capacity within minutes of receiving that message. Also, there was a significant jump in uucp and Internet traffic (painfully expensive to long distance uucp sites).

How can you protect yourself? If you're not running Erik's program, you are likely to be safe (check anyway to see if it has these same "features"). Modify your message bouncer to:

(a) Send a reply to one "Reply-To:" or "From:" address (the first From: address in the header seems logical to me).
(b) Don't send the entire message back, just the original header and a note saying "we got your message".

Paul pst!comdesign@pyramid.com ...!pyramid!comdesign!pst

Computing Down Under (Re: RISKS-6.94)

<willis@rand-unix.ARPA>
Tue, 31 May 88 17:37:55 PDT

I just returned from attending the IFIP/SEC-88 conference on the Gold Coast of Australia. It's a meeting that addresses protection of information systems in the broadest context. SEC-88 is the 5th in a series of roughly annual meetings, and is sponsored by TC-11, a technical committee of IFIP -- approximately the international analog of AFIPS.

In addition to doing a keynote talk on "Perspectives on Trusted Systems", one of the fun things for me was to participate in an evening public forum on social aspects of computer technology. In addition to myself, there were on the platform an Australian computer expert (who organized the conference) and two Australian politicians -- one a regional official of the Labor Party and the other, a present conservative Member of Parliament.

I had been cautioned that the subject would almost certainly center around the Australian ID card exclusively, and it did. By the by, the story that was told to me, and verified by something that I read down there, was that the only reason that the legislation did not go into effect earlier was that it contained a technical flaw; namely, in the haste of getting it ready, a switch-on date was inadvertently omitted from the law. This fact came from a prominent member of the Australian Computer Society.

The argument that developed during the evening -- and it apparently is the nub of the Labor Party position -- is that Australia has too much tax fraud [sic] and that the ID card is the answer. It seemed to me that the proper word was "tax evasion."

It seems that the Laborites feel that too much income is escaping the tax authority, and that it should be collected to make more revenue available for social and other programs. Obviously what Australia wants to do is corral the taxpayer, as the IRS does with its Taxpayer ID; Australia wants to be able to do the analog of tracking supplementary money flows as reported on the various form 1099s and similar documents here.

Other than the tax-related matter, no other argument was given for the institution of a universal ID card and number.

There was an amusing comment from the floor. A member of the Swedish delegation pointed out that Sweden has had a population register for decades, if not centuries, and Sweden has substantial tax fraud still.

My concluding comment was to point out to the Labor person that it seemed to me that he had a solution in search of a problem. In the best system-analysis tradition, I observed that the tax problem could very well be real, but that it looked as though it had been assumed that a universal ID was *THE* answer. There clearly are other answers and the government ought to do a more careful analysis of alternatives. Something in the spirit of the US/IRS arrangement would meet their tax needs, without subjecting the Australian population to all the RISKS associated with a

genuine universal personal ID.

The whole thing was covered by a TV crew whose interviewer chaired the session. I was told that a lot of air coverage was given to the occasion the following night, but I did not see it.

There seem to other RISKS in the Southern Hemisphere also; there has to be one somewhere in the following story. En route, I read an Auckland, NZ newspaper which reported a cable car incident. The Auckland cars are not in the spirit of the San Francisco ones but evidently more like an inclined railway running up and down a steep street in a more or less straight line.

Seems as though a cable car had crashed into a bumper at the end of the line with some injuries, but the RISK content is in the final words of the article:

> "The City Council had just spend [NZ]$90,000
> reprogramming the onboard computer."

Willis H. Ware, RAND Corporation, Santa Monica, CA

Computer Tampering Case to go to Trial

jcmorris@mitre.arpa <Joe Morris>
Tue, 31 May 88 17:29:53 EDT

Organization: The MITRE Corp., Washington, D.C.

From the _Washington_Post_, 31 May 1988, page D-1 (without permission, of course) comes the following article (credited to _Newsday_):

TEXAS TO HOLD A LANDMARK TRIAL ON COMPUTER TAMPERING BY 'VIRUS'

Texas prosecutors are preparing to go to trial in one of the first criminal cases in the nation involving spohisticated tampering with a computer's programming.

Donald Gene Burleson, a 39-year-year-old Fort Worth programmer, has pleaded innocent to charges of computer sabotage and burglary involving the USPA and IRA, Co., a Fort Worth-based insurance and securities concern. He is free on $3,000 bail pending a July 11 trial.

Burleson has lost a civil action in connection with the alleged 1985 computer tampering, and has been ordered to pay USPA about $12,000 in damages and interest.

Prosecutors charge that after being fired in September 1985, Burleson deleted records of thousands of sales commissions owed USPA employees from the company's computer system, and also introduced into the system a hidden program that would erase such data in the future.

Davis McCown, head of the Tarrant County district attorney's economic crimes

division, said in an interview last week that the program "had the ability to move through the [computer system], to change its name and to relocate."

[discussion of Trojan horses and viruses (virii?)]

[...] Burleson denied the charges and [said] that the company is blaming him for someone else's actions.

"They really have no proof," [his lawyer] said. "Anybody could have done the deletions" from the commission payment records.

Software can destroy hardware [From comp.sys.ibm.pc]

<ncar!ico!ism780c!microsof!danno@rutgers.edu>
Tue May 31 17:50:47 1988

Date: 24 May 88 01:49:55 GMT
>From uw-beaver!cornell!rochester!bbn!uwmcsd1!ig!agate!violet.berkeley.edu!willis Mon May 23 18:49:55 1988
From: willis@violet.berkeley.edu (Willis Johnson)
Subject: How did this program burn out two monitors?
Organization: University of California, Berkeley

I recently compiled a program that is supposed to do graphics on a Hercules graphics adapter. I've used a similar routine before, and I would have sworn there was nothing wrong with the software. Maybe the files got corrupted. When I ran the .exe file, my monitor made a high-pitched whine, then the power light went off, and a crackling noise came out of the back until I pulled the power cord. Curious about whether this was a coincidence, I took the program to work and tried it on an extra monitor I had there. The second monitor burned out too! I thought it was impossible to damage my monitor and adapter with software. Does anybody have any ideas what caused this? I'll post the .exe file and source (in C) to any brave or curious souls who request them.

The hardware:

1st time: homebrew PC clone with generic Hercules clone card
Quimax DM-15 amber monitor.

2nd time: Leading Edge Model D, "turbo" with built in
Hercules compatible adapter, Quimax DM-14
amber monitor (an earlier version of the DM-15).

Neither video adapter was damaged. Both monitors are DEAD.

Willis Johnson
willis@violet.BERKELEY.EDU
(415) 548 - 3023

>From uw-beaver!cornell!rochester!bbn!uwmcsd1!ig!agate!ucbvax!decwrl!labrea!glacier!jbn Mon May 23 22:29:15 1988
Path: microsoft!uw-beaver!cornell!rochester!bbn!uwmcsd1!ig!agate!ucbvax!decwrl!labrea!glacier!jbn
From: jbn@glacier.STANFORD.EDU (John B. Nagle)
Newsgroups: comp.sys.ibm.pc,comp.arch,comp.graphics

Subject: Re: How did this program burn out two monitors?
Date: 24 May 88 05:29:15 GMT
Reply-To: jbn@glacier.UUCP (John B. Nagle)
Organization: Stanford University

This is an old known bug. You can burn out the IBM monochrome monitor by stopping the horizontal sweep while keeping everything else running, and the Hercules card gives you enough control to do this under software control. The video chip lets you select the horizontal and vertical sweep rates independently, and zero rates are possible. However, the horizontal sweep is used as the oscillator for a switching power supply, as is typical in TV circuits, and with the sweep rate at 0, DC flows through a coil with high inductance but low resistance, producing an excessive current that burns out the coil.

Part of the problem is that the IBM monochrome monitor is a design lifted from an earlier, pre-PC product line, the IBM Displaywriter, and in that product, there was no potential vulnerability of this type.

Cash on the Nail, by Daedalus

Brian Randell <Brian_Randell%newcastle.ac.uk@NSS.Cs.Ucl.AC.UK>
Wed, 1 Jun 88 00:31:42 +0100

My original message to RISKS, with the copy of the Daedalus article, contained (or more exactly, since my files do not indicate one way or the other, I believe contained) an explanatory introduction about Daedalus, and his splendid articles. It was not my intention to test the gullibility of the RISKS readership!

Adding to the information that has since appeared about Daedalus:

(i) he is, I'm pleased to say, based here in Newcastle,

(ii) he has been claimed to be the world's most successful builder of perpetual motion machines! (A fascinating example, whose actual method of operation is still a matter of some mystery, is I understand in the Ontario Science Center, and

(iii) he was the subject of a splendid documentary on BBC TV recently, possibly in the Horizon series, which is worth looking out for, not least for its account of his perpetual motion machines.

Brian Randell

Re: Daedelus (RISKS-6.90)

Jacob Oestergaard Baekke <mcvax!iesd!jacob@uunet.UU.NET>
Tue, 31 May 88 14:08:10 +0200

> For years now, we have been told that the cashless society is

> just around the corner...

If this is the true condition of the cashless society in UK, you are behind the Danish banks. For the last one and a half year I have been able to do shopping and pay with my DanKort (in english: DanCard) which is the card you receive from your bank if you want to have a cashcard. In the Danish system all the banks has join forces and developed a system with a card with crypt 4 digit PIN code on a magnetic stip, a independent company runs the ATM automats, the pay terminals in the shops etc. The system operated on high security level; you get three attempts to enter your PIN code correct. If you has not enter a valid code the card is automatical blocked and you have to go to your bank, to raise the blockade. The obvious RISK in this system is if anybody place a fraud ATM which just read the content on the magnetic stip and the PIN code the custom taps in on the keyboard. But at present I have not hear anybody trying this.

Jacob Baekke, user of a DanKort.

Re: Down in the Dumps (dvk)

<srz@ATHENA.MIT.EDU>
Tue, 31 May 88 20:34:49 EDT

The Unix dump discussion illustrates having to balance two risks -- the risk of committing errors as an all-powerful superuser, vs. the risk of having an insecure system if access is improperly set for non-superusers. As pointed out by Brian Reid many months ago, giving system maintainers or administrators special privileges, such as write permission on system directories, has its own risks. Unix is a complex system, and setting certain protections has non-obvious side-effects.

For example, dvk advises that disks should be protected r--r--r--; in other words, everyone will have read access to the raw disks. This is equivalent to giving EVERYBODY read access to ALL files on that disk! In some environments, this may be ok, but other environments may want users to have some privacy.

Every site has to adopt some philosophy for dealing with Unix's all-or-nothing approach to privileges. I usually perform most system tasks as superuser, and after a long (and sometimes painful) learning process, I'm now careful enough not to destroy anything.

-stan

Down in the Dumps (a true story)

Mark W. Eichin <eichin@ATHENA.MIT.EDU>
Tue, 31 May 88 18:53:30 EDT

Dumps should be run as "sys", or some other non-priv userID. Disks should be owned by "sys", and protected r--r--r--.

Actually, r-------- is more appropriate... otherwise anyone who can
get to /dev (which should be *anyone* since /dev/null is in there) can
read the entire mounted disk, violating any security the filesystem
was meant to offer. Running a debugger with macros for opening up the
file system structure makes it easy to find files by hand...

Mark Eichin SIPB Member & Project Athena ``Watchmaker''

Down in the Dumps (a true story) -- OOPS!

<dvk@SEI.CMU.EDU>
Wed, 1 Jun 88 11:38:00 EDT

Oopsie, oopsie! I meant to say "protect you disks r--r------", but my finger
stuck and it came out "r--r--r--". If you do the latter, then anyone can
read you disks, which is not such a great idea. -Dan Klein

Re: Down in the Dumps (and not being root)

<dan@WILMA.BBN.COM>
Wed, 01 Jun 88 12:19:52 -0400

This message gives some very sound advice; one can, and should, avoid root
privileges if at all possible with UNIX. [... comment on r--r--r-- ...]

There are also problems with doing system administration as someone other than
root in a networked environment. Lots of people have their own workstations
and can configure them any way they like, pretending to be any user who might
have interesting privileges, like "sys". Sun's current version of NFS does not
perform any serious validation, so if you export a filesystem to my workstation
via NFS, I can read and write any file on it simply by setting up an account on
my workstation with the appropriate user-ID. The only exception to this is
root: an NFS client is never granted root privileges by an NFS server. So
there may be reasons why some things HAVE to be owned by root, even when it
would be better to avoid it, thanks to NFS. (Sun OS 4.0 apparently fixes this
problem.) In this specific case, I don't think device files can be accessed
under NFS (and you don't need to make the root filesystem exportable anyway),
but anyone trying this kind of thing should be aware of the general problem.

Dan Franklin

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 2

Thursday 2 June 1988

Contents

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

Happenstance and $70 Million

<Patrick_A_Townson@cup.portal.com>
Wed Jun 1 23:28:30 1988

On May 13, 1988, the day they allegedly embezzled $70 million from First National Bank of Chicago, two key players met in the waiting room at the Chicago & Northwestern Railroad Suburban Station.

Armand Moore, convicted swindler said by prosecutors to have masterminded the crime, was quick to assure bank employee Gabriel Taylor that the plan had gone off without a hitch.

"You did fine. Everything went great," Moore told Taylor. "Just sit tight. I won't forget to give you your share of the loot." Confident that all was well, Moore and the other co-schemers went out to look at new Jaguars and Cadillacs the next day.

But by Monday morning, May 16, the scheme had begun to unravel. Gabriel Taylor decided it best to begin cooperating with the government, and seven men, including Moore and another employee of First National Bank were indicted by a federal grand jury in the case two days later.

First National has said it anticipates no loss to itself or its customers

in the case. Although $19.8 million remained at large for several days following the exposure of the scheme, the bank has now retrieved it after filing suit against Citibank, which at first had refused to return it.

The effort failed 'only by the merest happenstance. This was a big near-miss,' according to Robert Edwards, a Hagerstown, MD consultant on money transfer security.

In the case at hand, about $70 million was sent out of the bank in just 64 minutes by wire transfer that Friday morning. Several trillion dollars per week is moved around the country by wire transfer, in which funds are moved from one bank to another by electronic debits and credits to interbank account at the institutions involved.

First National has been busily telling everyone who would listen that the attempt was foiled because of 'the effeciency of our system, and the many controls we use....'. Cynical insiders at the bank and members of the financial community in Chicago say that is nonsense. The scheme was a relatively simple minded one which failed because of the perpetrators' greed and apparent lack of sophistication.

"It's not the hackers and phreakers who are making trouble in most cases," said Edwards. "It's the employees who are working us over. When you have collusion between an employee and somebody on the outside, it is almost impossible to prevent fraud like this." He added, "The wire transfer business is extremely risky at best. This is one of the nightmares you live with."

In the First National case, the plot allegedly centered on Moore, known by his street name of 'The Chairman'. Moore came from his home in Detroit about the first of May to meet with his cousin Herschel Bailey of Chicago, one of those charged in the scheme.

Bailey knew Otis Wilson, who had worked at First National for six years in the wire room. He was also aquainted with Gabriel Taylor, another wire room employee. Both Taylor and Moore were low-level employees at First National. Both were young guys from the south side of Chicago who had gotten jobs at the bank as older teenagers a few years before.

There were several planning meetings at the downtown Quality Inn hotel, according to federal prosecutors. To entice the two bank employees, Moore flashed photographs of Rolls-Royce automobiles and luxury yachts, according to Assistant United States Attorneys Jeffrey Stone and Scott Mendeloff.

Moore allegedly promised Taylor and Wilson he would give them $28 million of the loot in exchange for their cooperation. At first, Moore wanted to steal $232 million, but Taylor convinced him that was just too greedy and risky.

Taylor and Bailey allegedly provided the others with confidential information regarding wire transfers, including the words and phrases bank employees would say to one another on the phone. They allegedly provided confidential information about the accounts of several large corporate customers of First National. They studied computer printouts to determine which of these various customers had the highest amount of protection against overdrafts, and which had the highest volume of transactions in their account, meaning that missing

funds would be difficult to immediatly reconcile. They rejected several of the accounts they reviewed, including Hilton Hotels Corp., for which the limits were too low.

The men allegedly selected three companies -- Merrill Lynch & Co,. United Airlines and Brown-Forman Corp. They called First National, purporting to be with those companies, requesting wire transfers. Taylor arranged to be the person who made confirming telephone calls, the government claims.

Under First National's procedures, the employee who receives the customer's request for a wire transfer cannot also be the employee who makes the confirming phone call. Furthermore, a third employee is required to actually operate the electronics involved in passing the money.

Prosecutors said the plan called for Taylor to hang up the phone if he was the person who received the incoming call. Calls to the wire room are routed automatically by a call distributor-like system; no one knows who will get which incoming phone call.

Keeping alert to the incoming calls, which were expected at certain times, Taylor then managed to get the task of making the callbacks, but instead of calling the actual companies involved, he called his accomplices at Bailey's house on the south side. Although the bank keeps a computerized record of all outgoing calls from phones in the wire room, the log was seldom checked and in any event was never checked immediately.

The money was transferred to accounts of Austrian banks at Chase Manhattan Bank and Citibank in New York that Friday morning between 8:30 and 9:34 AM.

Later Friday, Moore and another of his accomplices met with officials of another Chicago bank to discuss how they could move money from an overseas account and convert it to cash here in Chicago.

The scheme was derailed early Monday when United Airlines officials noticed a big overdraft in one of its accounts and immediately called First National. Brown-Forman did the same. What the schemers did not realize was that not only are the dialed digits recorded, *but the conversations are also*. They also did not realize that due to the size of the Merrill Lynch account, one employee at First National is assigned full time to handle only that account and attend to the needs of that very large customer. On coming to work Monday morning, the first thing that person did was review the latest printout for the customer. The overdraft was immediately noted, and since no other employee at the bank is ever authorized to debit or credit the customer's account or do maintenance on the account, it stood out like the proverbial sore thumb. A call to the responsible party at Merrill Lynch confirmed that they had not requested a transfer either.

Bank employees who wish to remain anonymous said it was naive to assume the large overdrafts would not be noticed in a matter of hours. "It's the greed that killed them," said one bank executive.

It's not really clear why the money was not moved out of the United States to the banks in Vienna on Friday rather than waiting for Monday. Although

the bank executive said the schemers were stupid about the whole thing, he admitted there were flaws in First National's system also. He said Taylor should not have been able to know for sure that he would be the employee to make the 'confirming phone call'. The person in the wire room who handles the confirmation should be selected at random just like the person who receives the call in the first place. The person actually doing the transfer should likewise be selected at random. By making it predictable to either party, a scam is that much easier.

The scheme would have eventually foundered anyway. You don't just withdraw $70 million from a bank in Austria without pretty thorough feedback and checking.

ABOUT THE DEFENDANTS - Gabriel Moore and Otis Wilson apparently had no prior criminal background. Both have elected to cooperate with the government in the prosecution of Armand Moore, a several times convicted con man. Both are free on recognizance bond pending their own trials. While its hard to feel sympathy for them, I *do* feel a twinge of sympathy. Both were (probably) very poorly paid clerks. They saw billions of dollars pass through their hands daily. When an older man, suave and sophisticated, takes them out to dinner, hovers over them, showers them with attention and offers to help them achieve the kind of riches they and their families could never legitimately have, it was too much temptation for them to resist. Wouldn't *you* find it hard? I know I would.... In all probability, based on the sentencing guidelines in federal court here, when they are tried, based on their pleas of guilt, the court will find them guilty. The government will make no recommendation as to appropriate punishment, and they will receive federal probation, probably for two to four years.

Obviously, they are blackballed from any further employment in banking/credit card/other financial operations. They face their families and friends as convicted felons.

If Armand Moore and his other associates -- the people who would have actually benefitted from the scheme (you don't *really* think they planned to cut those two kids in on it if they could help it, do you?) -- are convicted, most likely they will face hard time.

A curious dilemma arose regarding $19.8 million transferred to Citibank that Friday morning. *Citibank refused at first to give it back*. According to Citibank, all regulations regarding wire transfers were followed. The proper things were done, the proper words and phrases uttered, all was in order. Why, they asked, should *we* have to handle security at First National? They argued that wire transfers were intended to be immediate credits, and that if First National was now saying in effect that under some conditions their word on wires was not good, then why bother with a wire?

First National responded by filing suit the same day, Monday, May 16 in court in New York City, demanding that their money be returned to them. After some negotiations between Citibank and First National, *most* of the $19.8 million was returned. Citibank now says apparently they had better stop accepting wire transfers from First National altogether, or at least subject them to normal clearing procedures, for you never know when First National might come back a few hours -- or a weekend -- later and say it was in error.

Internal controls at First National have been so poor in recent years that in fact a lot of smaller banks throughout the country have begun holding their paper for clearance -- even cashier's checks and drafts -- simply because when 'errors' have occurred in the past, First National has taken what is percieved by many banks as a very uppity attitude toward investigation and restitution.

Mr. Edwards of Hagerstown called it 'sheer happenstance that it failed.' I think I agree.

Patrick Townson@cup.portal.com, PO Box 1003, Chicago, IL 60690-1003

(ps: Hinsdale seems to be rehabilitated - finally - as of the past few days! Rumors of terrorist activity/arson at the switch are totally unfounded.)

Re: Optimisers too tacit, perhaps?

Tim McDaniel <mcdaniel%uicsrd.csrd.uiuc.edu%uxc.cso.uiuc.edu@uxc.cso.uiuc.edu>
Wed, 1 Jun 88 12:23:33 CDT

>Does anyone wish optimisers were more forthcoming about the changes they make?

In general, I agree with your point. For example, some source-to-source parallelizing compilers can simply list their output; the output language is the input language, and often you can tell what input generated what output.

However, there are two possible pitfalls. One RISK is that if a compiler always puts out reams of messages, a user comes to ignore them, and may not notice the important ones.

Another problem is that super-optimizers super-mangle code. A change made by a super-optimizers after many passes may have little or no relation to the original source, and so a message may be totally inappropriate.

As one (possibly poor) example, consider the job of doing subscript checking in Pascal. Suppose that you already have a very good flow-analysis pass in your compiler. The straightforward approach would be to change

```
   var a, b: array [0 .. 10] of integer;
      i: 0 .. 255;
   ...
   a[i] := b[i];
into
   if (i < 0 or i > 10) then
      abort(some message about a);
   if (i < 0 or i > 10) then
      abort(some message about b);
   a[i] := b[i];
```

I say ``straightforward'' because these statements can be generated mechanically, yet it can be easily improved (if you have the good pass as above). A super-optimizer could remove the second ``if'', knowing that there is no return from abort and hence no path in which i is out-of-bound can reach the second ``if''. It could notice that ``i'' is non-negative and

remove ``i < 0 or''. If the original statement were enclosed in
for i := 0 to 10 do begin ... end
(a common case for arrays) then it could remove all the subscript-checking code.

The alternative would be to special-case the subscript-checking pass to insert the checks only when necessary. That would be far more error-prone and more specialized.

(There are many other optimizations that introduce dead code; see your local Dragon book. In fact, because users rarely write dead code, dead-code-elimination passes exist to clean up after the compiler itself.)

Alas, designing proper messages controlled by reasonable compiler options is not an easy task.

Re: Optimisers; Telecommunications Redundancy (Risks 6.94)

Michael Wagner +49 228 8199645 <WAGNER%DBNGMD21.BITNET@CUNYVM.CUNY.EDU>
Wed, 01 Jun 88 12:20

In Risks 6.94, J M Hicks <cudat@CU.WARWICK.AC.UK> asked:
>Does anyone wish optimisers were more forthcoming about the changes they make?

Yes, and for this reason, I've always liked the IBM translators, and particularly the PL/I optimising compiler. PL/I told you (as a warning-level message) when it detected and deleted unreachable code. PL/I also gave you a complete attribute and cross-reference list, marking the difference between reference and assignment. These are features I really miss in the C compilers I use now (including the IBM one, strangely).

I have had a number of philosophical discussions with people who feel that such functionality (a) does not belong in a timesharing or micro environment (because it produces long 'listings') and (b) does not belong in the compiler. While there might be a use for a tool that reads the defined reference language and produces such information (like LINT and XREF), I find it very useful when the compiler itself tells me. Amongst other things, it is reassuring me that it has the same understanding of the source code as I (and perhaps the reference language) have.

In the same issue, Klaus Brunnstein wrote:
> When analysing the missing redundancy in the ... `Deutsche
> Bundes-Post', ...
> our DATEX-P network has only one central communications controller
> per area. ... Despite many discussions and arguments ... the Post
> office managers argue that today, redundancy does not pay

To make this a little more concrete, here in Bonn, the central switch is in a little building on the banks of the Rhine. For a variety of reasons, the Rhine floods every year. The last two years have been particularly bad. Both Datex-P traffic and voice traffic in Bonn was badly hampered for days this year because of minimal redundancy. Nothing was done after last years flood, and I sincerely doubt that anything is being done about it now.

Michael

Major security hole in some sun systems

Jim Purtilo <purtilo@flubber.cs.umd.edu>
Wed, 1 Jun 88 13:07:19 EDT

We at UMCP have just discovered (the hard way) that there is a major security hole in a program called "rpc.rexd" on sun workstations. This program is intended to facilitate a form of remote execution between appropriate workstations; the front-end program which is used to request the remote execution is called simply "on". Unfortunately, "rpc.rexd" fails (miserably) in its check of whether the requesters should have the permission to do what they ask for.

Because of the way on/rexd works, anyone who wishes can, given root access to his own machine, become any uid he wants on any other machine running rex *anywhere on the Internet*. (Luckily, root appears to be the only exception to this rule, if that is some small consolation.) The authentication test in the Sun3.2 rex daemon appears to proceed as:

```
get the remote user id out of Unix-flavored authentication
if it's zero, then deny access
if getpwuid(remoteuid) is not NULL
   then grant access
   else deny access
```

In other words, any non-zero user identifier which happens to correspond to a valid user on the target machine can be used to gain the privileges of that user. There is no check to see whether that user has granted "trusted" status to the originating user and host (normally done via a file called ".rhosts" in many networked Unix systems), nor is there any check to see whether a system administrator has generically granted such a trusted status to the originating machine.

If you're running rexd and you're connected to a network, and if there are people or places on your net whom you don't trust, then we suggest not running rexd. To see if you are running it now, look in your /etc/servers table. If the "rpc.rexd" line is missing or commented out, you're OK. Sun does not enable this daemon in the /etc/servers you read off the installation tapes.

There are several ways that this problem seems relevent to the risks forum. The most obvious is the risk of blindly trusting a vendor to ship you software that performs at least `reasonable' security checks. We will not belabor that point here. Instead, we provide yet another testimony to how closely we must all watch what goes on our machines: innocent intentions can still lead to big headaches. Most of the Suns in our network ran version 3.0 of the Sun OS, served by a large central fileserver. Rex daemons were not readily available for this version, and there was no hole. However, many individual research groups have suns of their own. One day, a

guru running one of these individual Suns decided to be the first on his block to upgrade to release 3.2. He was not a staff member in our department, but was in fact trusted with superuser access to the fileserver. A well-intentioned chap, as he upgraded his owner's machine, he also installed the new, cute looking goodies from the distribution on the department fileserver so that all might benefit from his efforts. Hence, the normal scrutiny we would subject a new piece of software to was bypassed. Whether or not we would have found the hole when doing our normal installation of this software is unclear, to be sure, but we would at least liked to have had a shot at finding it. You can only speculate at where we have hidden the body of the late, otherwise well-intentioned, guru who installed the rex daemon.

Pete Cottrell, Steve Miller, Jim Purtilo, Chris Torek

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 3

Friday 3 June 1988

Contents

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

OTA Report: Science, Technology, and the First Amendment

<research!wolit@research.att.com>
Thu, 2 Jun 88 08:02 EDT

The U.S. Congress's Office of Technology Assessment (OTA) recently issued a special report that may be of interest to readers of the RISKS Digest. It is entitled, "Science, Technology, and the First Amendment," (OTA-CIT-369, Washington, DC: U.S. Government Printing Office, January, 1988, 73 pp., $3.50). The table of contents follows:

I. Freedom of the Press in the Information Age
  1. New Technologies for Gathering News and Information
     Newsgathering
     Computer Databases
     Media Satellites

Implications for Privacy
Implications for National Security
2. New Technologies for Editing and Selecting News and Information
Electronic Publishing
Editorial Control and Liability
Global Networks and the International Press
3. New Technologies for Publishing and Disseminating News and Information
The Convergence of the Media
Cable Television
Information Services Delivered Over Telephone Lines

II. Scientific Communications and the First Amendment

4. National Security and Scientific Communications
Science, Free Speech and National Security
The Executive Branch and Classification of Documents
Export Controls
5. The 1980s: Converging Restrictions on Scientific Communications
Contractual Restrictions on Communications
Restrictions on Informal Communications
Self-Restraint
National Security Directives and the Role of the National Security Agency
6. Constitutional Issues: An Overview

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

Disasters and computer facilities

Rodney Hoffman <Hoffman.es@Xerox.COM>
2 Jun 88 11:56:13 PDT (Thursday)

The 'Wall Street Journal' for Tuesday, May 31 features a story by Wendy L. Wall headlined "FEW FIRMS PLAN WELL FOR MISHAPS THAT DISABLE COMPUTER FACILITIES" (page 25 -- front page of Section 2). The lead sentence says, "Welcome to the era of the electronic disaster."

Starting with a review of the Hinsdale fire and its effects, the story discusses "accidents that disable the concentrated computer and telecommunications networks on which companies depend increasingly for basic tasks.... In a recent University of Texas study, 75% of businesses surveyed said they would have a 'critical or total loss of functioning' within 14 days if they lost their computer support.... Serious disruptions ... are becoming more common as computers spread...."

"Most businesses are ill-prepared to cope with electronic disasters, computer and communications specialists say.... Many top executives 'don't realize that the value of the information (in the computer) could very easily be worth several times the value of their hardware, software and building,' says Steven Christensen, a researcher at UT. In addition, the cost of insurance or backup

computer systems can be high...."

Besides dividing operations between several sites, the other major precaution taken by a growing number of companies is buying disaster insurance to use backup computer centers and networks: "The two largest disaster-recovery companies ... have nearly 1500 clients...."

The major example used in the story is that of wholesaler United Staioners, which has spent nearly $1 million a year on emergency preparations which served them well in the present Hinsdale fire: "Within hours, they dispatched a 31-man team, with backup data tapes, to an insurer's computer facility in New Jersey.... By the next day, they had reconstituted their entire computer network.... Although all this cost some $600,000 over two weeks, including a $40,000 fee for the insurer and travel costs for the 31 people sent to New Jersey, it probably saved the company at least $30 million in sales during that time, says United Staioners' CEO. Even more important, he adds, was the boost to customer confidence."

[Stationers? Stainers? Stallioniers? P.]

A few points from recent risks

David Herron <david@ms.uky.edu>
2 Jun 88 16:36:56 GMT

Running as root bad:

Someone from CMU berated the fella who'd messed up his disks for doing dumps as root and suggested instead running as "sys". hmm. My first thought was "what about files that people have protected against global reading? You'd need root to be able to read them". But dump reads directly from the device... no problem. I'd suggest a small change -- make the permissions "400" rather than "444" to prevent "everyone" from being able to read the disk.

In general however I've found it very good to engrave some of the more mystical and hard to remember incantations into shell scripts and the like. One of the first projects I did here was to come up with a backup procedure for our systems. I of course used shell scripts for the whole thing... I also put a sticker on the console giving the format of the backup command for those times when I was typing it directly, and relied on that sticker to jog my memory.

Multiple routes aren't multiple routes if they're the same physical route:

About the Hinsdale stuff. There were a number of trunks heading into the same building using the same exact physical route, right? And the claim was that the trunks were going over different routes. Well, this just isn't a very good assumption -- obviously. One only needs to remember the arpanet outage a year or so ago where a backhoe dug up some cables. All of New England's ARPANET traffic was ultimately routed through the cables that were in that one trench, yet they were separate cables going over different "routes".

sigh [See RISKS-4.30. PGN]

I think that we (as telecommunications customers) should have the ability to demand proper seperate routes (physical routes) for backup communications ...

Daedelus thumb stuff:

Um, joke or no I'm surprised nobody got scared over the same thing I was immediately scared over. That there's all these financial transactions sitting on my thumbnail and every time I purchase something I'm potentially telling the store all of my financial dealings for the past N months. That's a disclosure of information they have no need or right to know. Weell... they have a "need" in that it would give them a better idea of who they're dealing with, but I certainly don't want to be giving them such detailed information.

David Herron

Optimizing PL/I

Bard Bloom <bard@THEORY.LCS.MIT.EDU>
Thu, 2 Jun 88 23:22:40 edt

> Yes, and for this reason, I've always liked the IBM translators, and
> particularly the PL/I optimising compiler. PL/I told you (as a
> warning-level message) when it detected and deleted unreachable code.

The last time I used an IBM PL/I optimizing compiler (some years ago), I had a procedure which took two 32-bit integer arguments. I called it with the constant arguments 1 and 1. It produces some cosmically weird results. Eventually I put a print statement after the procedure entry; when the 1's got passed to the procedure, they were somehow transformed into 65536's.

Somehow the compiler was interpreting the 1's as 16-bit numbers and putting them in the wrong half of the 32-bit arguments. I immediately switched to non-IBM PASCAL.

-- Bard Bloom

Re: Auckland cable cars (Willis Ware, RISKS-7.1)

Richard A. O'Keefe <quintus!ok@Sun.COM>
2 Jun 88 07:38:09 GMT

It's about a year since I was last home, but Auckland didn't have any cable cars then, and I very much doubt that they've got any now. (The Museum of Transport and Technology has a small tram system, but those are old trams and have no computers.) There's a cable car in Wellington such as Willis describes, but then, Wellington is only the capital, can't expect people to get _that_ right. If the paper was the Sun, I've heard that it's typeset by computer, perhaps that is the risk story?

[Willis noted he read an Auckland newspaper. We'll assume the cable cars were really in Wellington, unless someone else contradicts it... PGN]

My experience with metal balloons

<edgerton%csdpie.DEC@decwrl.dec.com>
Thu, 2 Jun 88 14:26:20 PDT

About 2 years ago (Summer of 86) I bought a metallic balloon for my 2-year old daughter. It had a metal "string" about six feet long. When we were getting into the car, she let go of it, and it flew up into the corner of the parking lot and tangled up in the power transformer there. It shorted out the transformer and killed power for half the town.

After my initial surprise at the damage, and feeling lucky that I didn't have to pay for the damage, several thoughts crossed my mind.

1. That metal string should never have been used. Some powerline droop fairly low.

2. I jokingly told some friends that you could really "take out" the power of a town fairly easily. I was not aware how fragile our power system was.

3. The potential for mischief and vandalism implied by #2.

David J. Edgerton

Halon

Romain Kang <pyrnj!romain@rutgers.edu>
2 Jun 88 19:26:02 GMT

In RISKS 6.87, Anita Gould asks about dry-run tests of halon equipment. Here is a fortunate experience from such a dry-run:

To test that the equipment had been installed properly in a computer room, a gas other than halon was put in the tanks. The alarm was then triggered manually, and the room was evacuated.

Normally, the operator would have manually shutdown the system (Operating System, not power down), and then left the room. Since this was only a drill, the operator left immediately.

When we returned to the room, one of the 'dispersers' from the tank had shot itself across the room and was embedded in the wall. These 'dispersers' are cork-screw shaped metal objects, and have quite a point. In line with the trajectory of the disperser was the operator's chair at the console.

If the operator had actually stayed too long in the room to insure an orderly shutdown of the system, his own shutdown would have instead occured.

The tank was then turned to aim elsewhere, but the dispersers are normally not supposed to leave the tank.

Virus collection

<Robert_Slade@mtsg.ubc.ca>
Thu, 2 Jun 88 07:15:54 PDT

Re: my offer of the collected virus messages: please note that American postage is no longer acceptable. Send a 5 1/4" double sided, double density MS-DOS 2.xx or 3.x formatted 360K floppy diskette, with a self addressed *Canadian* stamped mailer to: Robert Slade, 3118 Baird Road, North Vancouver, B. C. V7K 2G6

Thanks to all of those who have followed the proper form. I hope the American stamped packages have not suffered too greatly at the hands of customs.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 4

Monday 6 June 1988

Contents

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

Review article on privacy/civil liberties risks in CACM

Jon Jacky <jon@june.cs.washington.edu>
Sun, 05 Jun 88 17:32:33 PDT

Many readers of this digest will be interested in the article, "Information technology and dataveillance," Roger A. Clarke, Communications of the ACM, 31(5): 498 - 512, May 1988. This is a long review with 78 references.

The author defines "dataveillance" to mean the systematic use of computing technology in the investigation or monitoring of the actions or communications of one or more persons. He distinguishes betwen "personal surveillance" - surveillance of an identified person, where there is a specific reason for the investigation, and "mass surveillance" - surveillance of large groups of people in order to identify individuals who might be of interest to investigators. The author concludes that computing technology is making it much easier to perform both kinds, a lot of it is going on and more can be expected.

The author says he does not argue that surveillance

is intrinsically evil or that it should be ruled out altogether, but argues that much of what is in fact now going on is in general a bad thing, especially the mass surveillance. He concludes that privacy and civil liberties protections in place in most countries are inadequate to protect against these new surveillance techniques. The author says that he feels people working in computing, due to their special knowledge, have some special responsibility to consider privacy implications of their work, evaluate safeguards, and lobby for effective ones.

- Jon Jacky, University of Washington

RISKS of wrong numbers and tigers

Steve Nuchia <nuchat!steve@uunet.UU.NET>
4 Jun 88 18:32:45 GMT

(Paraphrased from The Houston Post, 29 April)

A local newscast carried a story on a Herpes research project under way at Baylor College of Medicine, and displayed a phone number for volunteers to call - with appropriate assurances of confidentiality.

Not only was it the wrong number, it was the number for the "back door" to the public address system at Baylor (No indication of how large an area was covered - it is a big place.)

The callers, hearing a pick up but no answer "assumed it was an answering machine" and "gave their names, phone numbers, everything."

I believe this points up an important "human factor." People are a lot less cautious when they initiate a contact than when they are contacted. This explains the easy success of the typical "service spoof" attacks - password harvesters and "night deposit box out of order" scams. I don't have a magic answer for designers of services - it is very hard to design a service that is at all hard to spoof if the clients aren't at least a little bit cautious.

Second item:

One of the tigers went through a window in a door and killed an employee. It was at night and the public would not have been in immediate danger even in the daytime, but the incident nevertheless caused quite a ruckus.

The firm that designed the enclosure stated that the door design, including the window pane used, was "standard" for that kind of application. The tiger had no trouble going through it, and there was no indication that it was defective, nor that any other tiger would have had any trouble going through any other door of like design.

(Zoo officials have the big cats in holding cages while the window materials used in the (relatively new) cat facility are tested - by swinging miniature wrecking balls into them. The cat facility is a modern close-contact one - you

can routinely find one of the lionesses sleeping against a window with the public on the other side - in a tunnel.)

Apparently quite a few nominally professional people in the world think that standards excuse them from thinking. Perhaps that explains the popularity of standards?

Applicability to computers? Gee, there aren't any people clamoring for standards in the computer industry, are there?

Steve Nuchia uunet!nuchat!steve (713) 334 6720

[Yes, but we've always had tiger teams trying to break system security. PGN]

Academic Assignment of Viruses

<WHMurray@DOCKMASTER.ARPA>
Sun, 5 Jun 88 10:25 EDT

A society that depends upon any mechanism for its own proper functioning, cannot tolerate, much less encourage, any tampering with the intended operation of that mechanism.

Therefore, one is tempted to rise up in indignation at the idea of a qualified academic assigning a virus to his students. The next thing you know, they will be assigning plagiarism. How about the forgery of academic credentials? Perhaps we should offer a course in how to falsify research results. Or, perhaps, on how to trash another's experiments, notes or reports.

Perhaps it is a sign of immaturity that we are unable to recognize the moral equivalency. I will leave open the question of whether the immaturity is in the technology, the society, or academia.

I thought that we put this issue to bed several years ago when we stopped assigning the breaking of security. It seems that we did not.

For an academic to be unable to recognize that assignments, and the recognition that goes with their successful completion, encourages the behavior assigned, demonstrates a lack of understanding of the activity in which he is engaged. If he understands it, and still makes such an assignment, he demonstrates a lack of understanding of where his real interest rests.

Such irresponsible behavior may account, in part, for the anti-academic bias in our society and for the manifest distrust of the scientific establishment. It is of little wonder that the citizens of Cambridge, Massachusetts are reluctant to trust the likes of these with genetic engineering.

If there is any lesson that we should have learned from the computer, it is that understanding the effects of what we intend for it to do is a daunting task. Even getting it to do what we intend is not trivial. It seems to me, that there is plenty of material here for assignments; we need not look to assignments which are at best trivial, and at worst, dangerous.

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

Peter J. Denning on Terminology

Bill Kinnersley <iphwk%MTSUNIX1.BITNET@CUNYVM.CUNY.EDU>
Mon, 6 Jun 88 12:02:13 mdt

Subscribers to this list may be interested in the recent article "Computer Viruses" by Peter J. Denning in the American Scientist, vol 76 page 236. In particular, he discusses terminology. Paraphrasing his definitions:

1) Worm - a program that invades a workstation and disables it.

COMPASS '88 PROGRAM

Frank Houston <houston@nrl-csr.arpa>
Thu, 2 Jun 88 12:46:15 edt

```
        ****************************************
        *                          *
        *         COMPASS '88              *
        *    JUNE 27th - July 1st, 1988       *
        *                          *
        *    NATIONAL BUREAU OF STANDARDS     *
        *       Gaithersburg, MD           *
        *                          *
        *        ADVANCE PROGRAM           *
        *                          *
        ****************************************
```

* MONDAY, 27 JUNE 1988 *

Meeting of the Tri-services Software Safety Working Group

* TUESDAY, 28 JUNE 1988 *

0730 REGISTRATION
0900 CALL TO ORDER
General Chair---CDR Mike Gehl, Office of Naval Research
0910 OPENING REMARKS
Honorary Chair---Helen Wood, Deputy Director, Institute for Computer Sciences and Technology, National Bureau of Standards
0930 PROGRAM OVERVIEW
Program Chair---Janet Dunham, Research Triangle Institute
0940 INTRODUCTION OF KEYNOTE SPEAKER AND PANEL
Chair, COMPASS Board---H.O. Lubbes, Space and Naval Warfare Systems Command

0950 KEYNOTE ADDRESS
Chair, Keynote Panel---Dr. Roger McCarthy, Failure Analysis, Inc.
"THE PRESENT AND FUTURE SAFETY CHALLENGES OF COMPUTER CONTROL"
1100 COFFEE BREAK
1130 KEYNOTE DISCUSSION
PANEL: Herb Hecht, SoHAR, Inc.
Peter Neumann, SRI International
Jim Treacy, Federal Aviation Administration
Andres Zellweger, Computer Technology Associates
William J. Rodda, DELCO Electronics Corp.
1300 LUNCH BREAK
1430 RISKS AND BENEFITS
Chair---Janet Dunham, Research Triangle Institute
* "The Computer Related Risk of the Year: Computer Abuse"
Peter Neumann, SRI International.
* "Alzheimer's Patient Monitoring System"
Doris Rouse, Research Triangle Institute
* "Advance Computations into the Third Millenium"
James P. Farell
1530 COFFEE BREAK
1600 WHAT IS SOFTWARE SYSTEMS SAFETY?
Chair---Al Friend, Space and Naval Warfare Systems Command
* "Software Systems Safety and Human Error Avoidance"
Mike Brown, Naval Surface Warfare Center
* "A Definition of Process Security"
John McDermott, Naval Research Laboratory
* "Definitions and Requirements for Distributed Real-Time Systems"
Christina Berggren, IBM System Integration Division
* "An Approach to Software Safety Analysis in a Distributed
Real-Time System"
Sang H. Son and Chun-Hyon Chang, University of Virginia
and Paul V. Shebalin, ORI
1730 ADJOURN
1900 BANQUET
* "Stalking the Wily Hacker"
Cliff Stoll, Lawrence Berkeley Laboratories

* WEDNESDAY, 29 JUNE 1988 *

0900 RELIABILITY AND SECURITY OF VOTE COUNTING SYSTEMS:
Chair---Lance Hoffman, George Washington University
Panel: Roy Saltman, National Bureau of Standards
Emmett Fremaux, Jr., District Board of Elections and Ethics
Peter Neumann, SRI International
1000 ENGINEERING ERROR FREE SPECIFICATIONS
Chair---Sam DiNitto, RADC
* "Overview: Complementary Completeness"
Sam DiNitto, RADC
* "Early Detection of Requirements Specification Errors"
Paul C. Jorgensen, Arizona State University
* "Reliable Software Specification"
John McLean, Naval Research Laboratory
* "An Investigation of the Reliability of a Software
Specification"

Janet Dunham, Research Triangle Institute
1100 COFFEE BREAK
1130 DESIGNING SAFETY CRITICAL SYSTEMS
Chair --- Peter Neumann, SRI International
* "Designing Safety Critical Systems: The Viper Microprocessor"
Dr. John Cullyer, Royal Signals and Radar Establishment
* Question and Answer Session
1300 LUNCH BREAK
1430 SOFTWARE PRODUCT ASSURANCE: TECHNIQUES FOR REDUCING SOFTWARE RISK
Chair---Dolores Wallace, National Bureau of Standards
* "Software Product Assurance: Reducing Software Risks in Critical Systems"
William Bryan and Stanley Siegel, Grumman Corporation
"FIPS 132/IEEE 1012 SVV Plans Standard"
Dolores Wallace, National Bureau of Standards
1600 COFFEE BREAK
1630 VERIFICATION, TESTING, AND ANALYSIS
Chair---Michael Brown, Naval Surface Warfare Center
* "Predicting Computer Behavior"
Don Good, Computational Logic, Inc.
* "On Back to Back Testing"
Mladen Vouk, North Carolina State University
* "A Static Scheduler for the Computer Aided Prototyping System"
Dorothy Janson and Prof. Luqi, Naval Post Graduate School
* "The IBM Software Quality and Productivity Program"
Anne Martt, IBM Houston
1800 ADJOURN

* THURSDAY, 30 JUNE 1988 *

0900 SOFTWARE SAFETY MODELING AND MEASUREMENT
Chair---Herb Hecht, SoHaR
Panel: Jerry Mauck, Nuclear Regulatory Commission
Douglas R. Miller, George Washington University
Dev Raheja, Technology Management, Inc.
1015 USE OF MODELING TOOLS: A VARIED APPROACH
Chair---Don Lee, Aerospace Corporation
Panel: Sal Bavuso, NASA-Langley Research Center
Nancy Leveson, University of California-Irvine
1100 COFFEE BREAK
1130 PANEL DISCUSSION: SAFETY REVIEW PROGRAMS
Chair---George Finelli, NASA-Langley Research Center
Panel: Mike Brown, Naval Surface Warfare Center
Frank Houston, Food and Drug Administration
Mike Dewalt, Federal Aviation Administration
1300 LUNCH BREAK
1430 CASE STUDIES: OPERATIONAL SAFETY AND PROCESS SECURITY CONSIDERATIONS
Chair---Dan Strub, U.S. Air Force
* "On Software Safety Management"
Jim Dobbins, Verilog
* "A Methodology for Analyzing Avionics Software Safety"
Bob De Santo, LOGICON, Inc.

* "A Case Study of System Integrity for Alcohol Taxation"
T. F. Buckley, P.W. Garratt, and T.G. Gough, Leeds Univ., U.K.
* "Update on the Safety Verification of the B1 Bomber"
Joe Cantu, Boeing Military Airplane Company
* "The Centaur Project"
Helen De Mao, Corporation for Studies and Analysis

1600 BREAK

1630 CASE STUDIES: ASSURING MEDICAL SOFTWARE
Chair---Frank Houston, Food and Drug Administration
* "A Methodology for Assuring Medical Software"
Roger Fujii, LOGICON
* "Formal Safety Analysis and the Software Engineering Process in the Pacemaker Industry"
D. Santel, C. Trautman, and W. Liu, Medtronic, Inc
* Discussion/Question and Answer

1800 ADJOURN

* FRIDAY, 1 JULY 1988 TUTORIALS *

0900 Software Safety and Process Security in the Ada Reusable Software Environment
E.V. Berard, EVB Software Engineering, Inc.

0900 Verification and Validation
Dolores Wallace, National Bureau of Standards
and Roger Fujii, LOGICON, Inc.

1200 ADJOURN

REGISTRATION--Preregistration closes 17 June 1988. On-Site registration will begin on 28 June 1988 from 0730 to 0900 in the NBS Administration Building. Persons attending the Tri-Service Software Systems Safety Working Group may register there on 27 June 1988 between 1530 and 1730.

PARKING--Parking is available in the NBS Visitors Parking Lot adjacent to the Administration Building.

TRANSPORTATION--For those attendees who will be driving, the National Bureau of Standards is located on Clopper Road near the I-270 interchange approximately 12 miles north of I-495 (marked "National Bureau of Standards/ Clopper Road" for northbound travelers; or "National Bureau of Standards/Route 124 Darnestown" for southbound travelers). For attendees who do not wish to drive, the conference hotels are accessible from Dulles, National and BWI airports by regular limosine service with no reservation required. Also, NBS provides shuttle service to and from the Shady Grove Metrorail Station (on the Red Line) on the quarter and three-quarter hour (0815, 0845, ... 1715) from the West side KISS AND RIDE lot. COMPASS will provide a shuttle morning and evening between NBS and the conference hotels.

MEALS--The registration fee includes lunches on Tuesday, Wednesday, and Thursday, and Dinner on Tuesday evening. Refreshments will be available at all breaks.

FOR ON-LINE or hard-copy REGISTRATION FORMS, PLEASE CONTACT FRANK HOUSTON
houston@nrl-csr.arpa .

Halon agreement and the ozone models

Rob Horn <harvard!ulowell!infinet!rhorn@husc6.harvard.edu>
Thu, 2 Jun 88 19:31:50 edt

The real risk with the freon-halon-ozone controversy is best understood when you realize that the Third World countries were major opponents to the production freeze. The major uses of freons are:
1) Refrigeration
2) Manufacturing
3) Fire Protection (only about 10%)
Freons have been shown to be much cheaper and much safer than the alternative technologies. Only recently have there been indications that equally safe refrigeration technologies can be practical, and these will be many times more expensive.

In the Third World refrigeration means much more than a cool car. It can mean the difference between life and death. In food production, refrigeration allows produce to reach markets, to be stored safely. Without it (and most underdeveloped countries lack adequate refrigeration) food spoils, farm incomes drop dramatically, people go hungry, people starve. In medicine, refrigeration means medicines that don't spoil and blood transfusions. Lack of refrigeration means death. So the Third World countries opposed the removal of freons. Why agree to many thousands of deaths just to keep the Americans happy? The future environmental destruction is a good reason, but with so much at stake the evidence must be persuasive. Even with the new technologies, they must weigh the huge increase in costs against their limited incomes.

The evidence from the computer models is weaker than the press reports indicate. The measurements of world ozone show an *increase* of about 5% from 1960 to 1975 followed by a much larger and faster decrease of about 15% since then. The computer models do not predict or explain that increase. Their predictions of what altitudes would have how much of a decrease do not match the observed decreases. The models did not predict the Antarctic `hole', although this has a tentative explanation.

I believe that the real deciding factor was the intuitive decision by the negotiators that while the models were pretty inaccurate, the measurement data was accurate enough to make the trend very worrisome. The rapid action following confirmation of the satellite data calibration is consistent with this. It also is evidence of a cautious approach towards computer models. The

research level was dramatically increased, both into the atmosphere and into freon substitutes, after the initial modeling results were published. Freon uses with easy substitutions (spray propellent) were eliminated in the US. Oddly, the Europeans did not follow suit. The drastic changes were studied, but no action taken until there was much more information.

The Montreal agreement also places real emphasis on more data gathering and analysis following the agreed freeze and reduction in production. The reduction goal can be met with changes in refrigeration and manufacturing without any change in fire protection uses. The United States may move internally for much larger reductions. The large chemical companies may decide to switch production entirely when suitable substitutes are found. Dow has announced its intention to completely phase out freon production. The international agreement is to reduce somewhat, then wait for more evidence from measurements.

Rob Horn

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 5

Tuesday 7 June 1988

Contents

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

Re: Auckland cable cars (in Wellington) (Richard A. O'Keefe)

Mark Davies <ames!comp.vuw.ac.nz!mark@uunet>
Sun, 5 Jun 88 14:00:01 +1200

The cable car was in Wellington (in fact a guy in an office down the hall was waiting to catch it at the time and watched it go right past the stop and into the buffers at the end of the line). I had intended to post something at the time but the newspaper reports were pretty vague.

The cable car had only recently come back in service after its major yearly maintenance which apparently included a rewrite of its controlling software. The braking system failed to engage, and several people suffered minor injuries. The current status (several weeks after the accident) is that the cable car is still not running and samples of the code have been sent to the manufacturer, a European (Swedish?) firm.

This is from memory, more details when/if they become available. mark

---

Perfect computers

<HCART%VAX.OXFORD.AC.UK@CUNYVM.CUNY.EDU>
7-JUN-1988 09:32:02 GMT

The Sunday Times in the U.K. has produced, and is offering for sale, videos on microcomputing, because ''...there is clear evidence that British management has not yet appreciated the benefits of the microcomputer revolution.''

One of the benefits the Sunday Times has identified (June 5) is new to most of us reading the RISKS forum, I suspect:

''In the computerised office information, once entered, is always available....It is impossible to introduce an error, because the transaction is entered once only.''

The discovery by the Sunday Times of computers that can prevent entry of faulty data (provided, evidently, the entry is attempted once only), must be of interest to us all.

But what of those reading the article who might believe it ?

Hugh Cartwright, Oxford University.

Assigning viruses (RISKS-7.4)

Ian G Batten <BattenIG%uk.ac.bham.cs@CUNYVM.CUNY.EDU>
Tue, 07 Jun 88 17:46:49 BST

Talking of teaching virus-writing, WHMurray@DOCKMASTER.ARPA writes "The next thing you know, they will be assigning plagiarism. How about the forgery of academic credentials?"

One of the UK Polytechnics (virtual Universities) assigned a student exercise that was to break into some system (I seem to recall it was an 11/44 running V7) and assign yourself an "appropriate" mark. There was quite a row about it at the time (about two or three years ago). I'm afraid I can't recall any details beyond its being a London poly.

ian University of Birmingham Computer Science Department

Programmer sabotage

Bob Devine <devine%cookie.DEC@decwrl.dec.com>
Tue, 7 Jun 88 10:50:46 PDT

This is not really a "risk" but is yet-another case of increased legal definition of programming. Bob Devine

A programmer was found guilty under a Colorado law when he destroyed a program. A legal research company hired him to write a personal computer application that would permit a lawyer to search for relevant case law.

When a deadline was approaching and a leave request was refused, the programmer resigned, telling the company that they would never have the program. When the program could not be found on the system after he left, the company had to start over.

The programmer was found guilty of theft and computer crime.

First Interstate disaster planning and the L.A. fire (RISKS-7.3)

Jeff Lindorff <jeffl@sequent.UUCP>
6 Jun 88 21:09:37 GMT

The following is excerpted from an Associated Press article by George Garties. I can attest to the effectiveness of the measures described within as a customer of First Interstate Bank. Not once, in my experience, has a banking problem at my local branch been blamed on the Los Angeles fire.

AFTER THE TOWERING INFERNO, FIRST INTERSTATE DOSEN'T MISS A BEAT

Cole Emerson has known for two years that when the big earthquake hits California, it will be his job to get First Interstate Bank back into business.

When the city's worst high-rise fire swept the bank's headquarters last month, Emerson saw his disaster plans put to the test, and by all accounts, they passed.

[The May 4 fire gutted 4 1/2 floors of the 62-story building, killing a maintenance man and closing the building for an indefinite period of time.]

But by the start of banking hours the next day, the vital business of First Interstate Bankcorp, the nation's 9th-largest bank holding company, was proceeding. And only one of the company's 320 California branches was closed. The one on the building's ground floor.

Emerson, 42, is in charge of contingency planning and computer security. He is assigned to First Interstate Bank of California, although in the headquarters fire, his plan and staff also helped restart the parent company, which owns banks in 13 states and franchises in 10 others.

He recalled that shortly after the fire broke out, his five-member "business

resumption group" and a parallel group that deals with staff safety opened the bank's new emergency center in a computer operations building seven blocks from the downtown headquarters.

As damage reports came in, Emerson's group orchestrated moves for the vital groups that work in the headquarters.

They saw the securities trading department dispersed, with traders flying to company offices in Hong Kong and New York, as well as taking borrowed space in Los Angeles. They were prepared, since the disaster plan calls for traders and other key employees to carry home diskettes bearing vital records from their personal computers.

The main computers handling the bank's daily rush of consumer and business transactions weren't in the headquarters, but if they had been knocked out, they would have been backed up in Northern California.

The disaster plan was developed to deal with a great earthquake. The state Office of Emergency Services says odds are better than 50% that such a quake will hit the region in the next 25 years.

"An earthquake is real, and it's catastrophic, and it's going to happen," Emerson said. "There's nobody in my position in any of the banks who's going to say 'if.' It's always 'when it's going to happen.' I feel even more confident right now that we're well on the way to being prepared for that."

Jeff

(Not employed by Sequent Computer Systems, Beaverton, OR., so don't blame them.)

Telecommunications redundancy

Joel Kirsh <KIRSH@NUACC.ACNS.NWU.Edu>
Wed, 1 Jun 88 10:34 CDT

The mention of government involvement in assuring robustness of telecommunications jogged my memory. I recall reading of a particular U.S. government agency, which is solely responsible for taking control of telecomm services in the country in the event of a national emergency, to insure that the government's communications abilities are maintained.

The article went on to describe that the agency's control center was located within the blast radius of several primary nuclear targets, and no plans had been made to build redundant control centers.

Look and Feel Copyright Issue

Karl A. Nyberg <karl@grebyn.com>
Tue, 7 Jun 88 14:11:57 edt

Text of an article in the Wall Street Journal this morning. (I claim USC 17 in reproduction of this article for fair use, or whatever the appropriate

legal term is...)

This could have a chilling effect on the future development of software if the ruling is applied very broadly. I'm trying to get an actual copy of the specific ruling.

-- Karl, Grebyn Corporation, 703-281-2194 --

U. S. Agency Rules Software Copyrights Protect Displays on Computer Screens
By Bob Davis, WSJ, Tuesday June 7, 1988, p. 4.

WASHINGTON - The Copyright Office, in a boost to software publishers, ruled that software copyrights protect displays on computer screens from infringement.

Protecting software, either by patents or by copyrights, has been a muddled field of law in recent years. In a major case this year, Apple Computer, Inc. sued Microsoft Corp. and Hewlett-Packard Co. in March for copying certain graphical display features that Apple popularized in its Macintosh personal computers. An Apple spokeswoman, however, said yesterday's ruling doesn't directly affect that case.

Besides Apple, Lotus Development Corp. has tried to protect innovative computer displays by bringing copyright-infringement cases against competitors. But in cases of this type, it hasn't been clear whether copyright protection extends to instances in which companies, using different computer codes, generate displays that look like those of popular programs.

The Copyright Office, a part of the Library of Congress, rules that when a software company copyrights a program, it automatically copyrights the graphic and textual displays produced by the program. At the same time, the Copyright Office said publishers don't need to register any display or textual screen separately.

"We think the screen will be protected, no matter what the code" used to create it, said Richard Glasgow, the Copyright Office's assistant general counsel.

As an example, Mr. Glasgow said that if Apple copyrights its Macintosh software, the copyright "probably" protects the trash-basket symbol Apple uses to tell users how to discard files. Apple would only need to prove it has "an original drawing" of the trash basket to be covered by the copyright, he said.

... stock information ...

Decisions of the Copyright Office, which sets rules governing copyrights, are influential in federal courts that interpret those rules. Copyright protection lasts for 50 years after the death of an author or for 75 years if a company commissions the work and retains the copyright.

Jason Mirabito, a Boston copyright attorney, said the copyright decision gives "greater protection and certainty" to software publishers. Had the

Copyright Office required publishers to register every computer screen, he said, judges would likely have interpreted the protection narrowly to cover only exact copies of the disputed display screens.

But Mr. Mirabito said the broader copyright protection would likely encourage judges to rule that software publishers can protect their programs from competitors that merely "look and feel" like popular programs, but aren't exact copies.

However, computer veterans worry that if protection is extended too broadly, it may harm consumers and retard innovation, because it will slow the development of standardized displays. With such displays, computer users wouldn't have to learn a new set of commands with every new software program.

Moreover, "look and feel" cases are especially murky. If Shakespeare were alive, Mr. Mirabito speculated, he could have a copyright infringement case against "West Side Story" because it's very similar to "Romeo and Juliet."

The Apple spokeswoman said the ruling doesn't affect the suit against Microsoft and Hewlett-Packard, filed in San Jose, Calif., because Apple had filed separate copyright applications covering both the "literary and audio-visual" aspects of the display features it wanted to protect.

In its suit, Apple also accused Microsoft of exceeding the limits of licenses granted to it by Apple to use certain display features. At the time, computer industry analysts and intellectual property experts interpreted the suit as Apple's attempt to preserve a technological edge just as rivals were starting to close the gap.

[This case never ceases to amaze me, particularly in that much of the innovation came from Doug Engelbart's Augmentation Research Center at SRI in the 60's and 70's, and thence from Xerox PARC. PGN]

Risks of root typos

Tim Pointing <tim%dretor@uunet.UU.NET>
Fri, 3 Jun 88 11:42:32 EDT

In Risks v6n92, Dave Sherman <dave@lsuc.uucp> writes...
about accidental mis-use of dump wiping out a filesystem. The same sort of incident happened here earlier this year when somebody (who shall remain nameless to protect the horribly guilty [not me]) was running fsck on a PDP 11/70 running V7. This person's only mistake was leaving out a space. Instead of typing

"fsck -t tempfile /dev/rroot"

s/he typed

"fsck -ttempfile /dev/rroot"

(for those not familiar with the old fsck, the "-t" flag specified a temporary file for holding tables that grew too big for small address space machines). Unfortunately, this fsck came from well before the time

that "getopt" existed and manually parsed the arguments. It expected the temp filename as the argument after the "-t", not glued to it. The result was that fsck used the root filesystem device for its temporary storage (to ensure that the damage was severe, fsck starts by zero'ing the temporary file :-) and started checking a default filesystem. In the blink of an eye, the first 400 blocks of the filesytem were gone. Combine this typo with a flakey emergency system which, for reasons we have yet to determine, restored files incorrectly, and you can see that we had some *real* fun getting the system back on-line.

Tim Pointing, DCIEM

Access to DEC VMS 5.0 technical seminar

"Claude Barbe - SDR - (203) 431 5524" <BARBE%sdr.slb.com@RELAY.CS.NET>
Fri, 3 Jun 88 10:03 EDT

Working in the US under a 3 year L1 visa, I first could not enroll in the DEC VMS 5.0 technical seminar since I was not a US citizen nor holding a "green card". What surprised me is 1) the regulation that forces DEC to inquire about citizenship (the IRS is not that picky...) and 2) the menu system to accept my application could not handle L1 visa numbers...

Claude Barbe - Schlumberger-Doll Research, Ridgefield, CT

Risks of bank ATM cards (more) (RISKS-6.94)

Karl Denninger <mordor!lll-crg!lll-winken!ddsw1!karl@rutgers.edu>
Thu Jun 2 16:08:19 1988

Here's another risk in the use of the ATM cards:

At New Century Bank in Mundelein, IL there is an ATM terminal. About a month ago I used this terminal to make a sequence of transactions. The final transaction, a withdrawal of $20.00 was denied with a message "Cannot complete, try later". The card was ejected, with *no receipt* indicating failure. Thinking nothing of it, I went to another bank and obtained my cash.

About three weeks later the *same* thing occurred. Suspecting something funny was going on, I reinserted the card, and discovered to my horror that the ATM had indeed debited my account, yet not dispensed any cash -- AND NO RECEIPT.

This time I got a little peeved. The bank with the terminal (New Century) was unable to help at the time of the incident -- they claimed they had to wait for the "proof" from the machine the next day. My bank said the same thing.

The next day, my bank said that yes, indeed, there was a transaction recorded, and to their knowledge *it was paid by the machine*. They put in a charge-back request to New Century.

Upon more stringent questioning, they admitted that the charge-back might be

refused by New Century Bank, and that since I had no receipt to prove that the transaction failed, I could be out the amount of the transaction in question! (the card agreement clearly states that receipts from the machines are considered "official" evidence of a transaction or failure thereof, and that they are the *only* evidence which the bank will accept!)

I placed a call to "Cash Station, Inc" (the regional company handling the ATMs in this area) in an attempt to discover why the machines had been programmed to not issue receipts on failed transactions. Reaching someone with authority there took two days (!), and when I finally did get through the end result was that no change would be made.

New Century did eventually own up to having a problem -- in fact, they said that after investigation I was not the only one who had been "hosed". My questions were (and still are):

o Why was this not caught when the machine was balanced? It would seem as though if the machine recorded a debit of $20.00, and didn't issue the cash, that the machine would be out of balance by $20.00....

o After discovering that the machine was out of balance, why did New Century not attempt to rectify the problem themselves, or place the machine out of service until it was working properly? WHY DID THEY POCKET MY CASH?

o Why was a decision made to not issue receipts on denied transactions, and why does Cash Station, Inc. refuse to *require* that institutions issue these receipts?

o While I was on the phone with Cash Station, Inc. I inquired as to the display of balances (this was another "sticking" point with me; they were often off by hundreds of dollars). Their reply was that the network which interconnects the ATMs "cooks" your balance (!) depending on what you do at the terminal. In other words, the balance shown by the terminal MAY NOT BE YOUR TRUE BALANCE. When I asked as to why there was no indication anywhere that these numbers were "finagled" they indicated that the response time of the member bank's computers was insufficient to get a real balance.... sounded (and still sounds) fishy to me. Isn't this *literally* fraud, as they claim that number on the screen to be your BALANCE? (along this line, the machines do not dispense receipts on balance inquiries either -- perhaps to prevent you using these as "evidence".)

It would appear that someone (or many someone's) have been making out like bandits on these "failures" -- I was hit twice within 30 days, at the same terminal. How many others (who don't balance their checkbooks and thus never catch this kind of error) have also been taken for a ride?

What is most disturbing is that there was no indication that the problems would be resolved -- that is, no one was willing to state that they would begin (now or any time in the future) to provide receipts on all transactions in order to facilitate proof of what had occurred.

I have decided to boycott all ATMs in the Chicago area until I receive some satisfactory answers to these questions. So far no one has been able to

provide them. I suggest that others who are concerned for the safety of their funds also boycott the ATMs. Go to a Jewel (food store), where you can still use the card, yet you deal with a *human* who hands you your money.

Karl Denninger, Macro Computer Solutions, Inc. ...ihnp4!ddsw1!karl

---

Re: Australia Card [RISKS DIGEST 6.94]

Greg Bond <munnari!vertical.oz.au!greg@uunet.UU.NET>
Thu, 2 Jun 88 12:32:50 EST

This card was intended as a plastic card. I never saw any intention of a smart-card system. The initial idea came from the HEALTH department, as all eligible residents carry a "Medicare" card for the national health system. The Australia Card was to replace the Medicare card for the health system, and was also to be used for taxation, social security and other financial transactions. (For example, to open bank accounts, or start jobs, or employ brokers/agents, so any taxable transaction could be followed.) As the idea evolved, more and more departments and uses were included. I think over a dozen departments and 25+ "systems" were to have access to (part of) the database.

With 15M people, that is one ENORMOUS database.

The benefits the Govt. were flogging (and quite hard too) was savings on social security and tax fraud. (Numbers like $1b/year - about 2-3% of the Govt. budget).

There was to be a "Data Protection Agency" that was to monitor and control access to the sections of the database. No-one really believed it would work.

The idea was killed after the largest, loudest and longest public campaign I have seen. Many groups joined in, from the looney left to the radical right, including most professional Computing and Engineering bodies, as well as the obvoius civil liberties groups.

The RISKs? This proposal took on an awesome momentum, and grew frighteningly fast. I'm glad it was killed off before it started as unwinding or even slowing the increase would be enormously difficult. And governments aren't known for taking tough decisions.

One of the arguments in favour of the card was that with one centralised database, and legislative controls over access, we as citizens would actually be better off as far as protection and privacy were concerned.

Comments?

Gregory Bond, Vertical Software, Melbourne, Australia
Internet: greg@vertical.oz.au (or greg%vertical.oz.au@uunet.uu.net)
Bang: {uunet,mcvax,pyramid,mnetor,ukc,ucb-vision,...}!munnari!vertical.oz!greg
struct responsible for(these_opinions) { return me && !my_employer; }

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 6

Wednesday 8 June 1988

Contents

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

Buggy ATC Software

Paul Fuqua <pf@ti-csl.csc.ti.com>
Tue, 7 Jun 88 18:12:18 CDT

From the Dallas Morning News, June 7, 1988, without permission:

"Glitches" in a new computer program used by air traffic controllers at Dallas/Fort Worth International Airport can temporarily obliterate information on altitude, airspeed, ... types of aircraft in the area ... the call signs [,] and intended destinations of aircraft.

The same program is used at airports in Houston, Los Angeles, and Atlanta.

"When the program is running and it detects a glitch in the system ... it will remove the alphanumerics on the screen for a period of 20 seconds or less," said Lawrence Parrent, assistant air traffic manager at the D/FW Terminal Radar Approach Control center, or TRACON.

....

An audible alert is sounded when the data blocks are about to disappear, and FAA officials say the controllers have up to five seconds to either write down the information or memorize it.

Parrent said FAA officials do not believe the glitch constitutes a safety hazard. "The radar has not failed," he said. "The primary target is still there." The radar image and a four-digit number assigned to each aircraft remain on the screen.

....

Parrent said that the new program offers many features that improve the margin of safety in air traffic operations ...

[Discussion of potential problems if the "glitch" occurs during holding patterns or handoff from en-route controllers to approach controllers.]

FAA officials say controllers are able to determine the altitude of aircraft just as they did before the software was developed -- by asking the pilots.

[Comments from Parrent about controller uneasiness.]

[Testing began in January, increased to 24-hour-a-day use after April.]

"The reason we are testing with live traffic is that we do not have the capability to simulate the number of targets in off-line conditions," Parrent said. "We have to test under actual conditions.

"It's like other aviation-type equipment -- just like an airplane. You put it in a wind tunnel and it looks great, but you still have to go out there and put a test pilot in it and fly the darn thing."

End of article.

Comments:

The system itself is obviously aware of a problem, or it wouldn't be able to sound a warning. Wouldn't it be better to leave the information on the screen, even if updates are frozen until the 20-second problem is over? Even if the only benefit is to avoid disturbing the controllers? And "up to five seconds" to record information on "up to ten" aircraft? (The number's in the article, I just omitted it.) Did anyone ask the controllers what *they* would like to see in the new program?

The FAA apparently considers this a minor problem because when it fails it's just equivalent to the old system. What about (a) becoming dependent on the new features and (b) the "startle factor" when the warning sounds? Did the problem show up before the peak-period testing? If so, how come it hasn't been fixed in five months, and if not, isn't that an extra worry?

Since I'm working on simulations and simulators at the moment, I can sympathise with the inadequacy of off-line testing, but I'd rather the field-test were on something less important than an air-traffic control system. Sounds like a good argument for better simulation technology and more computing power to use what's already there.

Paul Fuqua, Texas Instruments Computer Science Center, Dallas, Texas

The Challenger and visionary software architects

Kent Stork <stork@humu.nosc.mil>
Tue, 7 Jun 88 12:37:37 HST

The May issue of Defense Science validates something that many computer scientists have probably suspected: ultimately, the failure of the Challenger and the death of the astronauts was due to a control loop software design oversight - just another bug.

To what extent must software architects be visionaries? Certainly the requirements are proportional to the power of the system the software controls. Do such visionaries exist to design our Challengers and our other more aggresive weapons?

How To Stop A War (Dunningan and Martel)

<mnetor!utzoo!henry@uunet.UU.NET>
Wed, 8 Jun 88 00:45:16 EDT

Of some small relevance to Risks, and of possible interest to readers, is a recent book: "How To Stop A War", James F. Dunnigan and William Martel, Doubleday 1987. The authors are military analysts, not peace marchers. A good look at the realities of why wars start or don't. (Sample: "As long as there have been technically complex weapons, there have been accidents. For example, one sixth of the losses of modern battleships were due to accidental explosions. If such a formidable ship can accidentally demolish itself, it's no wonder users are fearful about the safety of current systems... During the 1986 Air Force raid on Libya, two F-111 aircraft were needed for every one that got through in working order to drop its bombs.")

Henry Spencer @ U of Toronto Zoology {ihnp4,decvax,uunet!mnetor}!utzoo!henry

---

UK Poly; another root typo (RISKS-7.5)

Matt Bishop <bishop@bear>
Wed, 8 Jun 88 08:02:36 EDT

The UK Polytechnic that Ian Batten was talking about is described as case 78.066 in the book "Computer Insecurity" by Adrian Norman (Chapman and Hall, New York, c. 1983, p. 191.) This book, incidentally, is an excellent collection of incidents involving computer security (or lack thereof) and even does some analysis to show some things that lead to security problems. (The computer was a DEC10 system, not a PDP-11/44; other than that, though, the details are exactly the same.)

Yet another root typo story: a certain person who had superuser privileges once accidentally typed "exit" rather than "halt" to leave superuser mode. The former does just that; the latter halts the CPU ...

Matt

Re: The Australia Card [RISKS DIGEST 7.5]

Amos Shapir <nsc!taux01!taux01.UUCP!amos@Sun.COM>
8 Jun 88 05:32:25 GMT

Israel does implement a system of a national ID card, used by all government agencies, banks, hospitals, employers, etc. There is no central database (yet!) but information cross-over is relatively easy.

Last month a man requested for a loan from a bank; his request was denied because (the bank claimed) he had just applied for the same type of loan two years ago. Checking it out, the poor guy found out that there was another man with a similar name, who had the same ID number, and what's more, the other guy was a criminal wanted by the police.

It seems that the criminal had lost his ID card a few years ago, requested a new one, and the Ministry of the Interior had issued him a new one - with the other man's number! They claim that since the system has been computerized by now, such a mistake cannot happen again...

Amos Shapir, National Semiconductor (Israel)
6 Maskit st. P.O.B. 3007, Herzlia 46104, Israel Tel. +972 52 522261

Re: Risks of bank ATM cards (more) (RISKS-6.94)

John Pershing <PERSHNG@ibm.com>
8 Jun 88 08:32:35 EDT

In reply to Karl Denninger's posting...

I don't see any risks in his story that can be attributed specifically to the use of ATMs, as opposed to the more general use of a Bank. If anything, the risk is assuming that a transaction that is "untouched by human hands" will be less likely to go wrong when, in fact, it is more likely to have something go wrong.

Specific points:

- The error undoubtedly *was* caught when the machine was counted out at the end of the day (assuming that your bank follows accepted accounting procedures).

- They didn't know it was "your cash". The machine ended up the day with too much money, which means that one (or more) of the 500 people who used the machine that day got short-changed. Undoubtedly people were assigned to look into the problem if it has happening on a regular basis (probably a mechanic was sent out to clean and oil the ATM).

- I have never gotten a receipt for a failed transaction. Requiring a receipt for a failed transaction sounds sort-of bogus to me, as one of the (dozens of) failures that can happen is that the receipt printer breaks or runs out of paper.

- There is no such thing as a "true balance" from the bank's point of view, as you undoubtedly have a bunch of "paper" (checks, credit charges, etc.) floating around that they haven't seen yet. Also, contrary to popular opinion, electronic funds transfers are seldom posted against the "bank of record" in real-time -- rather, they go onto a tape somewhere and get fed in at night. So, any "balance" that your bank would report is necessarily flakey.

  Indeed, there are response-time requirements placed on banks that are wired in to ATM networks (typically a few seconds). Since the "real" records are on a tape in the back room, the "front-end" computer only has your balance as of last night (or, maybe the night before) plus the electronic transactions that it has seen go by. It may have missed some electronic transactions, e.g., due to crashing and/or a network failure. It hasn't seen any of the day's paper. The electronic transactions that it has seen haven't been verified yet.

Electronic banking systems are incredibly complicated. It is impossible to even imagine the number of things that can go wrong, or the number of ways that clever consumers can subvert the system. Of course, this is nothing new with ATMs -- financial fraud has been around as long as banks. It is quite sensible for an ATM's programming to "lean" in the bank's direction is there is something amiss, because the consumer will always go complaining to a bank officer. When was the last time that you got *over*-changed and actually reported it?

Go ahead and boycott the machines if you want. However, if you want them to improve, then you have to exercise the system so that the bugs will be found and fixed. If your bank is not responsive to your bug reports, then find another bank.

John Pershing, IBM Research, Yorktown Heights

ATM risks - the figures in UK

Alasdair Rawsthorne <alasdair%unix.cs.man.ac.uk@NSS.Cs.Ucl.AC.UK>
Wed Jun 8 14:19:19 1988

I have always refused to possess an ATM card, on the grounds that the individual is not well protected against the banks' errors, particularly since bank employees perceptions of the possibility of malfunctions differ from mine.

My feeling has been strengthened in the past by one or two highly publicised cases of the banks' intransigence in the face of complaints of ``phantom'' withdrawals from ATMs.

I've not seen a case of this type now for a few years, and was beginning to succumb to the idea that the safeguards have improved, when I came upon an article describing the UK Banking Ombudsman. He is the arbiter of last resort for customer complaints, and will only accept cases that have exhausted the relevant bank's internal complaints procedure (usually at general manager level).

According to Money Management(June '88), the Banking Ombudsman received 198 complaints in March 1988. The category with the highest number of complaints was.....

``Cashcards - unauthorised withdrawal'' with 17 (~9%) complaints.

Are there any figures for other countries banking systems?

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 7

Friday 10 June 1988

Contents

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

Accidental breach of software security

Martin Minow THUNDR::MINOW ML3-5/U26 223-9922 <minow%thundr.DEC@decwrl.dec.com>
9 Jun 88 16:08

From Electronic Engineering Times, June 6, 1988, condensed and abstracted.

Unauthorized access to software cited
Shuttle security lapse
by Richard Doherty

An accidental breach of software security at Rockwell International Corp.
gave unauthorized engineers and programmers access to raw code being prepared
for the space shuttle Discovery's return to space, now slated for Aug. 22.
The six-month lapse in security resulted from "an unintentional keyboard
error," Last November, the most recent embodiment of "Operational Increment"

shuttle software (revision OI8-A) was somehow stripped of its normal RCAF [Resource Access Control Facility] protection... [IBM] Engineers discovered on Nov. 22, 1987, that they were able to modify the code while in the supposedly restrictive "browse" mode. An IBM supervisor then immediately notified NASA, and by afternoon's end, a weekend-long bit-by-bit comparison was initiated.

NASA says that in all, 16 changes were made. The agency still does not know by whom or when. Because multiple copies of the OI8-A software existed at that time, NASA said there is no chance the security breach could endanger the mission.

NASA conducted a six-month long inquiry into how the event happened. As a result, the agency said it now knows the normal protection was somehow stripped off during a change in editing modes (between integer and block) and who the operator was at the time.

But NASA said it still doesn't know how many accesses were made and by whom over a six-month period. Nor has it discovered why it took six months to notice the code was open to editing.

Shuttlegate?

The acknowledgement by NASA and Rockwell engineers came in the wake of a $5.2 million lawsuit field by shuttle engineers who were dismissed after expressing concern about overall OI8-A software vulnerability, among many other problems, to Rockwell management last fall.

The engineers, Sylvia Robins and Ria Solomon, first took their concerns to the company's ombudsman, then to the NASA Inspector General and, eventually, to the White House.

Finally, seeing no action taken on their concerns regarding accelerated software verification audits and a steady lack of secure data access, Robins and Solomon took action by filing a lawsuit here [Houston] against Rockwell and its prime software contractor, Unisys, last fall. That action triggered widespread denial by Rockwell of the lawsuit's many safety concerns, including the charge of lax shuttle programming security that was finally acknowledged last month.

[There's more, but this is getting long. Any idea what "between integer and block" modes mean?] Martin

---

"Sewage flows into river; Computer Failure Blamed"

Randal L. Schwartz <mipos3!merlyn%intelob.Berkeley.EDU@ucbvax.Berkeley.EDU>
Tue, 07 Jun 88 10:34:13 PDT

Page one (below the fold) of the 6/7/88 morning edition of The Oregonian (Portland, Oregon) reports:

[BEGINNING OF ARTICLE]

"Sewage flows into river; computer failure blamed"

* The five-hour spill from the Sullivan Pump Station poured about 5.4 million gallons into the Willamette River downtown

A computer failure caused about 5.4 million gallons of raw sewage to spill into the Willamette River in downtown Portland early Monday, prompting state officials to warn against recreational use of the river through Tuesday morning.

"That's a major spill," said Shirley Kengla, spokeswoman for the Oregon Department of Environmental Quality.

[What a quote! We Oregonians now know what a major spill is... sheesh.]

The spill began about 3 a.m. when a computer failure at the Sullivan Pump station caused sewage to flow directly into the river [...]. The spill was stopped by 8 a.m. [...].

Peterson [operations director] said the computer failure was caused by a loss of electrical power, shutting down the pumps at the pump station.

He said the computer system was designed so that the operators could override computer commands at the station, but they discovered Monday they could only do that when the computer had electrical power [!!!]. Monday's loss of power prevented that.

[... more stuff about volume and repair efforts ...]

Kengla said the DEQ is investigating the spill.

"Because it was a computer failure, it was an accident [!!!] and for that reason, we're just looking toward making sure it doesn't happen again," she said.

[... more stuff about location of spill ...]

Contact with the water could cause sickness with severe flu-like symptoms.

In June 1985, another computer failure caused the dumping of more than 3 million gallons of raw sewage into the Willamette from the same pump station. Kengla said that state and city officials had been working to prevent a recurrence of the problem.

"We thought we had done enough, but obviously we hadn't," she said. [Brilliant quotes!]

[... stuff about another tiny spill last year, not computer-related...]
[END OF ARTICLE]

(1) Why did they have a computer-controlled system that depended on

electrical power to operate with no backups?

(2) Given that they already had a failure before, how could they have failed to design a failsafe system?

(3) The statements made by the spokeswoman, like "because it was a computer failure, it was an accident..." make me wonder. Why should an accident be so obviously required to happen after a computer failure? Why should we not *plan* for the system to break? These guys obviously didn't.

Sheesh. And during Rose Festival too!

-- Randal L. Schwartz, Stonehenge Consulting Services (503)626-6907
on contract to Intel Technical Publications: merlyn@omepd.intel.com (for now)

[Moderator's note: This article was also reported by Andrew Klossner <andrew%frip.gwd.tek.com@RELAY.CS.NET> and by Richared {?} England, Mentor Graphics Corp., Customer Services, Technical Support, Beaverton, Oregon, pdx.MENTOR!rengland@uiucdcs. The abridged version from Randal was chosen for brevity, but the following comments from R. England are also worth including:

> [This case] points out, once again, the need for total design consideration. A truly fail-safe system would include manual overrides instead of requiring all control signals to originate from the automatic control system. Conversation with the writer lead me to believe that there was a wide-spread power loss which may have precluded operation of the pumps as well, in which case nothing would have helped. Note, however, that the computer gets the blame. [R. England]

Canadian Public Service warned against SINing

John Coughlin <JC%CARLETON.BITNET@CORNELLC.CCS.CORNELL.EDU>
10 Jun 88 10:25:00 EDT

The following article appeared in the Ottawa Citizen, Friday June 10, and is reproduced without permission.

==========

PS warned against SINing

By Iain Hunter
Citizen staff writer

Treasury Board President Pat Carney has ordered bureaucrats who run hundreds of federal programs to SIN no more. And Justice Minister Ray Hnatyshyn has warned that the government may bring in laws to regulate the collection and use of the social insurance number if other levels of government and the private sector don't follow the federal example.

Carney announced Thursday that the use of the individual identity number will be phased out over five years in several institutions to reduce the risks of invasion of [...] privacy. Carney said the use of the SIN will be restricted mainly to the administration of tax, pension and social benefit programs. Any new collection or use of the SIN beyond those covered under the new policy will have to be approved by Parliament.

A Treasury Board spokesman said "hundreds" of programs in which the number is now used will be affected by the new restrictions. The cost of phasing out the use of SIN is estimated at $16 million.

Privacy Commissioner John Grace called Carney's announcement heartwarming and said it puts the federal government "in a much stronger moral position to preach controls on the use of SIN to other governments and the private sector."

Betting network crash in Australia

George Michaelson <munnari!ditmela.oz.au!G.Michaelson@uunet.UU.NET>
Thu, 09 Jun 88 09:40:23 +1000

Earlier this week (Monday) the T.A.B suffered a major loss of a computerised betting control system which caused much anguish to punters across the state of Victora. I phoned their computer manager & got a loose description of the problem, he was understandably reticent since the network manages many millions of dollars of bets daily, and there are public relations issues aside from the security ones.

Brief Description of TAB & Gambling:
++++++++++++++++++++++++++++++++++

Gambling, the 4th most ancient vice after programming sex, religion and politics is endemic in Australia. It is also very tightly controlled by the state, concentrating in several HUGE casinos with banks of "pokeys" or one-armed bandits, and of course the ponies. [remember phar lap anyone?]

Apart from pre-computed instant win cards and lotterys the only [legal] form of betting off the racetrack in Australia is run by the T.A.B. or Totalizer Agency Board.

They run a "totalizer" scheme, where the pool of cash placed in any given race is split into the dividend, so that the winnings are more "socially" adjusted, and also not simply calculated from starting price ("SP" bookmakers thrive in the better drinking establishments and police stations, according to popular myth & corruption tribunals) however there is an element of feedback, in that offered "odds" are obviously adjusted according to the poolsize as well as traditional form, much as in normal betting. the "divi" depends on the size of the pool and is post-close-of-betting calculated, although a running total could be available (I don't know for sure, I'm not a gambling man you understand...)

Each state has a transaction processing network which underpins this exercise, so that the pool/dividend holds across the entire state for each race.

The Problem:
++++++++++++

The Victorian T.A.B. uses a tightly coupled "cluster" of 5 nodes handling the incoming transactions, and a central node that acts as a controller and calculates the divi. Some form of shared memory is used to do all this.

At some stage in the day the central node noticed an inconsistency in 2 separate pools, across two of the nodes. They were disconnected, possibly automatically. Afterwards, the entire network was taken down and the betting calculated manually to prevent any data inconsistency being propagated out into the real world. -From the "feedback"-y nature of the tote algorithm it's plausible that had this not been done, many many thousands of punters would have been rooked of their winnings.. actually perhaps they would have made too much money as well!

-The problem was verbally ascribed to software, but no details are available. According to radio reports over $1M was lost due to the much less efficient manual methods. Punters were furious.

I wanted to end with some pun about shutting the sTABle door after the horse has bolted, but I can't think of a good punchline.

George Michaelson, CSIRO Division of Information Technology

ACSnet: G.Michaelson@ditmela.oz Phone: +61 3 347 8644
Postal: CSIRO, 55 Barry St, Carlton, Vic 3053 Oz Fax: +61 3 347 8987

John Pershing on ATMs

David Thomasson <ST401405%BROWNVM.BITNET@MITVMA.MIT.EDU>
Thu, 09 Jun 88 09:38:27 EDT

A tip of the hat to John Pershing (pershing@ibm.com) for his reply concerning risks of ATM's (RISKS 7.6). This piece is truly a standout in that it is (a) not anecdotal and (b) not hysterical in tone. I commend it to others as a model for crafting their arguments and replies.

A typo in "UK Poly; another root typo" (Re: RISKS-7.6)

Matt Bishop <bishop@bear.Dartmouth.EDU>
Thu, 9 Jun 88 09:01:57 EDT

Error in my last letter: he typed "halt", not "exit"; "halt" halts the CPU and "exit" takes you out of superuser mode. Sorry for the boo-boo. Matt

Re: The Challenger and visionary software architects

Eugene Miya <eugene@amelia.nas.nasa.gov>
Thu, 09 Jun 88 16:16:29 PDT

>From: stork@humu.nosc.mil (Kent Stork)
>The May issue of Defense Science validates something that many computer
>scientists have probably suspected: ultimately, the failure of the Challenger
>and the death of the astronauts was due to a control loop software design
>oversight - just another bug.

I have grabbed the May issue of Defense Science (an oxymoron):

%A Yale Jay Lubkin
%T The Challenger Disaster
%J Defense Science
%V 7
%N 5
%D May 1988
%P 13-18 (actually only 3 pages)

This article neither validates nor mentions software, bugs, or computers.
There are two sets of problems 1) Kent's comment, and 2) the article itself.
The article is basically a summary of different causal hypotheses: the
cold joint and the AW&ST puncture (Abu-Taha) hypotheses. There is a good
tone of conspiracy in the paper, but I am not in a position to side in
defense of Washington bureaucrats or Lubkin.

The closest comment to "control loop software design" is:
> "It was not the leak that killed the astronauts. It was the
> attempt to correct the sidethrust, which sent the Challenger
> into violent oscillations.

There are probably some difficulties in asserting "cause." Further:
> "If the Challenger had been permited to go off course,
> without attempting the major correction, the side booster would
> not have broken out, the booster would have burnt out with the
> Callenger still intact, and the crew could have ejected, off
> course but aslive."

This latter is probably false, but we will not really know. I don't usually
trust words like "ultimately."

Researching this article did have a positive side benefit while in the library,
I found a good 5 page obit to Richard Feynman in Engineering and Science
[Caltech's Alumni magazine].

There is a very "hardware must fly" orientation in NASA, and you should
understand software is not well understood in the Agency.
This was documented by internal reports [Sagan et al. 1980].
Any disaster will have underlying PHYSICAL causes sought.

>To what extent must software architects be visionaries? Certainly the

>requirements are proportional to the power of the system the software controls.
>Do such visionaries exist to design our Challengers and our other more
>aggresive weapons?

I take some offense at you calling the Challenger a weapon, and I know several thousand others who would, too. I would not call any of the software people working on the Shuttle "visionaries," there is a degree of salesmanship, however. Your codes have to withstand many walk throughs (or walk overs depending on your prespective 8-). Don't think the control problem scales linearly, it doesn't, typically O(n^2) and greater.

--eugene miya
NASA Ames (not speaking directly for the Agency)

COMPASS '88 CONTACT

Frank Houston <houston@nrl-csr.arpa>
Fri, 10 Jun 88 16:51:28 edt

Regarding the COMPASS '88 advance program and registration info.

Some people have had trouble contacting me by email and I, in turn, have had some difficulty getting the nrl-csr mailer to recognize return addresses. I recommend including a surface mail address with requests for registration info. For those who could not reach me by net, my telephone number is (301)443-5020. Registration is still open.

Frank Houston (I really exist @nrl-csr.arpa)

[Note, not on the foregoing, but on the following:
I have had a request to add the issue number on the standard trailer, as you see I have done. That seems like a fine idea for people who tend to string RISKS issues together. However, this may defeat the UNDIGESTIFIER programs if they look for the precise trailer. Please let me know if this causes any troubles. PGN]

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 8

Thursday 16 June 1988

Contents

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

New Jersey wants computer audit trails disabled

Joe Morris (jcmorris@mitre.arpa) <jcmorris@mitre.arpa>

From _Computerworld_, 13 June 1988, p. 4 (without permission, of course):

> CASINOS FIGHT PLAN FOR COMPUTER ACCESS
>
> Atlantic City -- In a major dispute over government access to corporate computers, 11 Atlantic City casinos are fighting a proposal by the New Jersey Division of Gaming Enforcement (DGE) to obtain direct access to casino computers for investigations.
>
> Unfettered computer access is necessary to fully investigate and regulate

> casino operations, DGE officials say.[...]
>
> The casinos have been joined in their battle by privacy experts, who say the proposal would set a dangerous precedent by allowing government agents to go on secret "fishing expeditions" through business computers. Public comments on the proposal are due this week.
>
> [discussion of parallel paper-and-electronic records, due process requirements, etc...]
>
> The proposed regulation, published last month and pending before the state's Casino Control commission, would require the licensed casinos to provide DGE investigator with inquiry-only access to ALL [emphasis supplied] computer records.
>
> The requirement would have the following conditions:
>
> * The New Jersey casinos must provide the DGE with an on-site terminal and the capability to make printouts.
>
> * DGE personnnel must be given "reasonable privacy in which to conduct such inquiries."
>
> * Casinos may not track or monitor the DGE inquiries, and casino computers must be programmed to preclude any such tracking.
>
> * Casinos may request a log of DGE inquiries that shows the general category of information examined and the time of the inquiry.
>
> * Each casino must train DGE personnel in the use of its computer system.
>
> [The DGE tried to get this done four years ago but was blocked by a court order requiring extensive hearings. DGE changed the procedures under which the demands were made, prompting] an April 7 filing by 11 of the 12 Atlantic City casinos [which] raised numerous objections and argued that the new proceeding defies the 1985 court order.
>
> [discussion of the loss of audit trail info for inquiries, which would make it impossible for anyone to know if compromised information had been leaked by a DGE employee or someone else.]

Wow. Regardless of one's stand on how deeply the Mob owns the casinos, you've got to wonder just who if anyone at DGE knows how to spell "Computer Security". After we've been careful to build security audit capability into systems (and screaming about how dumb designers of the older systems were for not doing so), now comes DGE with orders to shut them down. Anyone want to give some odds on some other part of DGE filing charges against the casinos for failing to maintain an audit trail of access to the detailed profiles they keep of the high rollers?

Disclaimer: the odds are very high that you won't be able to show any link between yours truly and any casino or the DGE, mainly because there isn't any. Of course, we all know how easily computer records can be changed...

Bunkers

C H Longmore <CCAse7-16%UK.AC.BIRMINGHAM@CUNYVM.CUNY.EDU>
Wed, 15 Jun 88 19:23+0100

The following is from The Independent of 15th June 1988, reproduced without permission.

* * * *

COUNCIL WAR BUNKERS HIT BY COMPUTER PROBLEMS

The Home Office has suspended installation of a critical part of the Government's wartime communications network, a multi-million pound computerised link-up for local authority bunkers.

A national programme for the installation of the County Message Switch system was halted at the end of March because of "Software Problems"

The Home Office confirmed yesterday that the software was still being tested.

One county emergency planning officer has privately described the situation as "an absolute botch-up".

Bunkers in Lancashire, North Yorkshire, Cornwall and Somerset have been affected by the delay following extensive teething problems encountered during a pilot installation in Bedfordshire.

It is understood that the system's memory specifications are so limited that district computers can only take about eight messages before previous files are automatically deleted.

One source said yesterday that the Home Office had suggested that punctuation and spaces should be left out of messages in an attempt to avoid overloading the system. But there have been complaints that this would make messages more difficult to decipher.

There are also complaints that because of a lack of back-up batteries, a power cut would result in the computer system's entire memory being automatically wiped out. [Note: bunkers have their own generators, but EMP from a nuclear airburst could easily disrupt the supply]

* * * *

[Note: In the UK, the Civil Defence plans in time of war are to keep the population in the towns and cities where they live, and devolve power to Emergency Regional Seats of Government if central Government is incapacitated.]

One of the thoughts that occurred to me was this:

Why upgrade from teletypes to a new [?] computer system. After all, the

message capacity of a teletype in that of the roll of paper attached, and they don't need rebooting after a power failure. You can also read them in the dark by using a torch. If you were getting really technical you could use an incoming teletype, and outgoing terminal/teletype.

And another one was:

Upgrading this sort of computer system is very dangerous. The more complex the technology involved (ICs, DRAMS, Magnetic Media etc) the more prone it is to damage from ElectroMagnetic Pulse from Nuclear Weapons, fluctuations in the generator supply and other adverse operating conditions. A simple teletype is less technologically advanced and therefore probably *more reliable* in these conditions.

And finally:

Is this going to end up as another Nimrod fiasco, where the UK government spends millions of pounds on a system, and then scraps it and buys from the US instead?

-- -- --

C H Longmore: CCAse7-16%bham.ac.uk@cunyvm.cuny.edu

More on Blackhawk helicopter

Dave Horsfall <munnari!stcns3.stc.oz.au!dave@uunet.UU.NET>
Fri, 10 Jun 88 16:42:13 est

From "The Australian" 31st May 1988:

"German incident sours Blackhawk shield plan

The United States Army says it will speed up plans to shield the UH-60 Blackhawk helicopter from radio-wave interference following an incident in West Germany earlier this month [May]. On May 11, a Blackhawk flying near a large group of powerful antennae banked into a right-hand turn for five seconds without any pilot commands.

[...] An Army spokesman, Major Phil Soucy, said on Friday that tests had shown the problem of electromagnetic interference did not jeopardise flight safety. ``We certainly are not going to ground the (Blackhawk) fleet because there's no reason to'' Major Soucy said. He said the Army had begun talks with the helicopter's manufacturer, Sikorsky Aircraft, on shielding a number of electronic components.

[Details on Knight-Ridder report of 5 accidents and 22 deaths, since 1982]

The Army and Sikorsky, a subsidiary of United Technologies Corp of Hartford, Connecticut, disputed that report, saying there was no evidence that electromagnetic interference had caused any crashes."

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

---

root typos

Ken Yap <ken@cs.rochester.edu>
Fri, 10 Jun 88 17:55:24 -0400

You don't even have to be root to wreak havoc. I have the escape character in rlogin set to ^P because I want to keep ~ for my own use. One day I was using the console on a Vax to make a backup tape and logged in to another machine to read my mail while waiting. When I decided to escape back to the Vax to check how the backup was going, I got:

<>>

(For those not familiar with Vaxes, this is the bootstrap prompt.) Fortunately I realized that I had halted the machine and typed C <return> immediately.

These days I do one of the following:

(1) Ensure the console switch is on LOCK.
(2) Avoid using the console.

Ken

---

costs/risks of impregnable telephone booths.

Geoff Goodfellow <geoff@fernwood.mpk.ca.us>
Mon, 13 Jun 88 11:56:59 PDT

The following was passed to me from David Kucharczyk <ssr@cos.com>: Taken from the Sydney Morning Herald and the May 22, 1988 issue of Awake magazine.

In an effort to outwit phonebooth thieves, Telecom, Australia's government-owned telephone company, has fitted the susceptible booths with Kirk safes. Named after the worker who invented them, the safe has so far proved 100-percent effective. As mentioned in the Sydney Morning Herald, it has withstood 'oxy torches, ramset guns, angle-grinders, hydraulic jacks, pulley clamps, centre-punches and bricks.' Ironically, the new safes appear to have led to an increase in vandalism, as theives frustrated by the tough safes vent their anger on the booths. Telecom reports that the current rate of smashed glass and ruined handsets and cords is at a new high of 3,000 cases per month.

[note by Geoff: reminds me of the time my car was broken into in an unsucessful attempt to steal the stero/casette player. the shattered glass everywhere, the mangled radio face plate, storage of the car in a secure

location until i could obtain an appointment at the fix-it shop, the overhead of taking the car in / pick-up, etc -- all besides the expense/insurance deductable. quite a hassle, for which i would have given the radio away to have avoided!]

Science, Journalism, and Whistle-Blowing

<mnetor!utzoo!henry@uunet.UU.NET>
Fri, 10 Jun 88 18:05:34 EDT

The following is the editorial by Daniel E. Koshland Jr. in the 29 April 1988 issue of Science; it has relevance beyond the scientific community. [Reprinted (sigh) without permission.]

"Discussion of fraud in science is becoming a cottage industry in need of an environmental impact report. Fraud is devastating to science; it undermines the basic respect for the literature on which the rapidity of scientific advance depends. It must be rooted out wherever and whenever it is discovered. That makes it all the more imperative that charges of fraud be made responsibly and that the performance record of whistle-blowers be scrutinized as well as those of the scientists they criticize. In recent times we have been exposed to excesses in whistle-blowing and journalism that come close to the evils they wish to eradicate. We see, for example, the charge that there is widespread fraud, followed by a text defining fraud as a broad concept including "misconduct". Misconduct is then interpreted to include such items as poor proofreading or incomplete references. In a recent congressional hearing, misconduct was further broadened to include a difference in interpretation of complex data. Crying wolf tends to lose effectiveness when the wolf is redefined as a vicious mouse and then it is further conceded that the viciousness is a matter of opinion.

"The slowness of institutions in conducting investigations is viewed by some as evidence of an "old boy" conspiracy. But there are good reasons to be slow to accuse a colleague. A student works in close cooperation with a professor for months or years and finally solves a problem. A statement by the professor that "we can't publish until the result is checked" might eliminate a few cases of fraud, but it would forever damage the relation between student and professor. Institutions that are quick to accuse distinguished faculty members of misconduct or worse on the basis of gossip or flimsy data will not long have a distinguished faculty. The fate of whistle-blowers who have lost their jobs or failed to continue in science is often recounted as evidence of retaliation, but the quality of the whistle-blowers' work is relevant to this conclusion. The idea that scientists may cut corners to achieve fame, but whistle-blowers never do, is nonsense. Past track records are not always a guide to future conduct -- some distinguished scientists err, some erratic whistle-blowers are right on occasion -- but scientists, like ordinary citizens, are innocent until proven guilty. Investigation of their integrity should require substance. It is not a cover-up for an institution to refuse to initiate an inquiry if the only evidence is the accusation by an unreliable source.

"The scientific apparatus cannot afford to disregard accusations of fraud,

and competent whistle-blowers help science. Investigations should be pursued meticulously, but the final report should strongly state the outcome: If the accusation is correct the miscreant should be punished and the whistle-blower commended. If, however, the accusation is incorrect, in addition to the usual bland announcement of exoneration there should be a denunciation of the false charges and a documentation of the time, anguish, and delay that has been occasioned. Science cannot tolerate fraud, but it should not be at the mercy of headline-happy journalists or incompetent whistle-blowers.

"Journalists must distinguish between fraud, sloppiness, and differences of opinion. When an accusation of fraud is made, if the evidence appears weak or the charge exaggerated a careful journalist should be alerted to probe more deeply. Opinions of noninvolved experts on the likelihood of error and the track record of the accuser should be documented early on, even in the initial story. The original story may have to state the facts of an accusation before all the background is obtained, but in most cases the story can be delayed, and in all cases pertinent doubts should be expressed. The final outcome should be publicized appropriately. Finally, the setting in which a story is reported must be considered by a journalist. A story involving a prominent scientist in an inquiry on fraud is bound to make headlines, even if the story is only a question of judgement. The late Senator Joseph McCarthy was particularly clever at manipulating journalists in this way; the techniques should be familiar by now.

"Scientists respect integrity, scholarship, and good judgement as much as they abhor fraud, sloppiness, and poor judgement, but these are very different phenomena. Those who mix them together in uncritical ways may decrease our chances of eliminating true fraud, may damage reputations unfairly, and may diminish enthusiasm for healthy differences of opinion at the cutting edge of science."

Henry Spencer @ U of Toronto Zoology
{ihnp4,decvax,uunet!mnetor}!utzoo!henry

Shrink Wrap

<WHMurray@DOCKMASTER.ARPA>
Wed, 15 Jun 88 09:41 EDT

Yesterday I received an unsolicited package in the mail. From the source and the marking "magnetic media," I conclude that the package contains a program sent to me for evaluation and review.

I am usually cautious about unsolicited mail. However, this one came with its own warning. It was sealed with a sticker with the following warning: "The program on the enclosed disk is licensed to the user. By opening this package, you indicate your acceptance of the ENCLOSED (emphasis mine) license agreement."

Goodness! What might I be agreeing to? The fantasies are simply endless.

Hard-disk risks from vendors

Jerry Harper <mcvax!euroies!jharper@uunet.UU.NET>
Wed, 15 Jun 88 15:41:59 GMT

We use a number of 286 machines (American Research Corporation -made in Taiwan) for some development work before uploading the code to an MVS/XA environment. REcently, one of the machines has given considerable trouble and, indirectly, an insight into the obligations of the vendor we dealt with. The system unit emits quite a noticeable vibration which transmits itself forcibly to the keyboard and desk - that problem has been there from its purchase. On several occasions the vendor has checked the unit to ascertain the source of the vibration but to no avail. Almost from the start I mentioned that the vibration was bound to cause some damage to the hard-disk in the long run (increased oscillation of the heads,etc). In the last month one of the crimped connections to the hard-disk controller board fell out with the result that drives C and D were not recognised and some 30mb, it appeared were either lost or inaccessible. I took the shroud off the unit and pushed home the connector - we lost two recent files (yes, we have floppy backups). A week later the same occured only but this time I couldn't locate any loose connections, so I rang the vendor. Firstly, he said he was too "busy" to come out, and then he told me in a matter of fact manner that the hard-disk was probably corrupt and all the data was lost. We have had this machine *four* months. He then proceeded to give a telephone analysis of what might have happened. Eventually, I was tiring and demanded that someone appear quickly. Two days later a technician came and once again it turned out that a power connection to the the hard-disk had worked itself loose. At this point, I decided that we should have a replacement machine. No dice. I was assured that the machine was in fine form. A week later the CMOS went sick and the hard-disk was inaccessible. Once again a telephone analysis was conducted and I reconfigured the system. I know this is getting long-winded but the point is that at no stage in any of the exchanges did the vendor admit any liability, nor did he seriously offer a replacement. This is of some concern to a number of companies here in Ireland as quite a number of vendors have suffered financial difficulties leaving their customers with pitiful after sales support. Are too many people getting into the VAR market by the seat of their pants?

Jerry Harper : Merrion Gates Software (Logic Programming)
: 89 Booterstown Avenue, Blackrock, Co Dublin, IRELAND.
Phone-net : 353-1-88 52 51
email : jharper@euroies.uucp

An old CTSS virus

<garyt@cup.portal.com>
Mon Jun 13 11:42:06 1988

SENT: 88-06-11 19:00

FROM:2 VANVLECK_TOM @PRUNE

This may qualify as one of the oldest viruses: Just before the July 4th holiday in 1966, two undergraduate CTSS users decided to write a RUNCOM (like a shell script) which would invoke itself. They knew that this would create a new SAVED file on each invocation and eventually use all the disk space on the Project MAC CTSS system, but they thought this would just lead to a documented error return. Unfortunately, there was a bug in the system and CTSS crashed. Noel Morris and I spent a long time repairing the system disk tables by hand. Well, was this a virus? The program launched a new copy of itself, and this proliferation led to the death of the host.

(Note the early fascination with self-reference. The other well-known way to crash CTSS was to issue the XEC * instruction, which said "execute the instruction at the location where this instruction is." The 7094 CPU looped taking I cycles only and couldn't be interrupted. Bill Matthews once did this deliberately to stop the system when an unwary system administrator accidentally put the password file in the "message of the day." Once again, at 5PM Friday.)

The most important lesson is "don't get clever at 5PM Friday."

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 9

Wednesday 22 June 1988

Contents

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

Risks of ATM manufacturers

"Philip E. Agre" <AGRE@AI.AI.MIT.EDU>
Thu, 9 Jun 88 02:05:54 EDT

In reading Risks over the last couple years, I've noticed that responses to attempts to complain about uncorrected technical problems tend to take certain recurring forms. John Pershing's message about ATMs illustrates a remarkable number of these forms of argument, all of which will be familiar from previous Risks discussions of related topics, such as privacy violations and whistle-blowing at NASA.

What has happened? Someone, in this case a customer though in other cases it has often been an employee, complains that something is badly amiss with some system, receives no redress, and finds that their reports are ignored. So they make noise about it. The response?

1. Misplaced accusations of uncooperativeness. `You have to exercise the system so that the bugs will be found and fixed.' The person

has exercised the system and discovered and reported difficulties with it, but the organization in question ignored the reports and thus (we must presume) neither found nor fixed any bugs.

2. Condescending lectures about how `incredibly complicated' the systems in question are and how hard it is to anticipate all possible problems. Nobody has demanded that all problems be anticipated, only that attempts be made to repair detected problems, especially ones that cause unnecessary loss or injury.

3. Misplaced appeals to the market. `If your bank is not responsive to your bug reports, then find another bank.' The ATM didn't just have a bug, it stole this person's money. And presumably it is stealing other people's money. Why doesn't the knowingly misdesigned software constitute a company policy to defraud its customers? And don't ATMs, as a legal matter, fall under some version of the notion of implied warranties of merchantability?

4. Casting misdesign as an irremediable act of God. `It is quite sensible for an ATM's programming to "lean" in the bank's direction is there is something amiss ... .' Wouldn't the really sensible thing be to make a record, whether on a paper receipt or in a computer file, and preferably both, that something was amiss in this particular transaction?

5. Diagnosing the system is the victim's job. `... the consumer will always go complaining to a bank officer. When was the last time that you got *over*-changed and actually reported it?' It is even more sensible to "lean" in the customer's direction, because the bank will always be motivated to fix problems that cost it money. When was the last time a bank discovered it had over-changed you and actually let you keep the money?

6. This-is-nothing-new. `I don't see any risks in his story that can be attributed specifically to the use of ATMs, as opposed to the more general use of a Bank.' Such a statement requires that we define the problem far too abstractly. The story concerned a particular misdesign. Taking it as an abstract attack on ATMs misses the point.

7. Blaming the victim. `It is impossible to even imagine ... the number of ways that clever consumers can subvert the system. Of course, this is nothing new with ATMs -- financial fraud has been around as long as banks.' A customer gets defrauded, yet somehow the issue has gotten twisted around into customers committing fraud. Note the irony of the last bit: banks have committed financial fraud as long as there have been banks.

Risks of bank ATMs

Mary-Anne Wolf <MWolf@BCO-MULTICS.ARPA>
Thu, 9 Jun 88 11:38 EDT

The ATM itself is not all that you need. Baybanks in (Eastern) Massachusetts has a dial-less telephone next to their ATMs, which reaches an office staffed 24 hours a day. I have only used this phone for information, but I assume that, if anything went wrong, it would be possible to inform someone and check the state of the machine immediately. If the bank decided to wait until business hours to check the machine, they could still have a record of who claimed to be short-changed. These ATMs also have a camera behind glass pointing at the customer, and although I never know when it's running, it seems unlikely that someone would fake a complaint. One pays for this convenience with relatively high minimum balances and relatively low interest, but, as long as I have the money, it's worth it. (When I didn't have the money, I got a better deal at a bank with only 2 branches that didn't offer ATMs at all, and a check-cashing card in a 24-hour supermarket for emergencies.)

I suspect that the problem is less the machine than the attitude of the bank. A bank should probably rather risk losing a little money than a lot of customers, and I would boycott banks rather than ATMs if I boycotted at all.

Mary-Anne Wolf, MWolf -at BCO-Multics.ARPA, Honeywell Bull, Billerica MA
These opinions are my own, and my only connection with any bank is as a customer.

Re: Risks of bank ATM cards

Larry E. Kollar <dcatla!mclek@gatech.edu>
Fri, 10 Jun 88 16:43:31 EDT

>From: John Pershing <PERSHNG@ibm.com>
>
> - I have never gotten a receipt for a failed transaction. Requiring a
> receipt for a failed transaction sounds sort-of bogus to me, as one
> of the (dozens of) failures that can happen is that the receipt
> printer breaks or runs out of paper.

The ATMs around Atlanta always give you a receipt, whether or not your request went through. Usually they have a code on the front, with a list of codes and what they mean on the back.

As for the printer breaking or running out of paper, it's not a hard thing for an ATM to detect the lack of paper flow and put itself out of service. Whether or not ATMs do that is yet another question.

Earlier, Karl Denninger relates that the bank told him "no receipt, no fix." ATMs keep an internal printout of account numbers, as an audit trail. It came in handy for us a couple of years back when my wife deposited $400 in cash, threw the receipt away, and the ATM crashed that evening and forgot to transmit the transaction. We didn't know what had happened until checks started bouncing on us. This safeguard must be on all machines; Georgia isn't much of a consumer-oriented state to require that kind of special modification.

Larry Kollar ...!gatech!dcatla!mclek

Yet more on the Blackhawk helicopter

<wolit@research.att.com>
Fri, 17 Jun 88 10:15 EDT

Additional details on the incident Dave Horsfall reported in RISKS DIGEST 7.8, from 'Aviation Week & Space Technology,' June 13, p. 31:

> The most recent tests were conducted near a dense antenna field of nearly 1 sq. mi. that radiates on a broad range of frequencies with a power level
>
> potential well above 400 MW, according to Army officials. During the tests, the aircraft experienced uncommanded rudder pedal movements that caused the UH-60 [Blackhawk] to begin turning, stiffness in the rudder pedals and illumination of caution and advisory lights in the cockpit.
>
> Specifically, the test UH-60 experienced a simultaneous loss of hydraulic pressure to both tail rotor servos for approximately 5 sec. and a jamming of the tail rotor control pedals. Both malfunctions were attributed to the susceptibility of the hydraulic logic module to the high energy levels. As a result, the service has decided to accelerate the hardening of the module for both production and retrofit as the first priority under the modified ECP [Engineering Change Proposal 384].

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

Re: root typos

Dave Curry <davy@intrepid.ecn.purdue.edu>
Thu, 16 Jun 88 12:49:07 EST

Ken Yap relates his problems with ^P and the Vax console. Fortunately, ^P is not the standard rlogin escape.

Here's a better (worse?) one: the console escape character on the CCI Power 6/32 ("tahoe") is the tilde. And, so is the escape character for Berkeley mail. You guessed it... log in on the console, send some mail, and do a "~h" to see the headers.... ooops, the machine just halted.

CCI also cleverly placed the "reboot" switch, an up/down toggle, on the front of the cabinet, not recessed, and at knee level. Fortunately, UNIX seems to ignore the switch.

--Dave Curry

P.S. - Don't get me wrong; the tahoe is a really *nice* machine, regardless of the above demonstrations of poor design judgement.

Another Root typo

<nyssa@terminus.att.com>
Fri, 10 Jun 88 13:59 EDT

This has taken on an almost urban legendary status in our group:

Four summers ago, we were doing a beta test at a customer site.
Our field support person had to remove some files in a directory, so
he had to use the "su" command. This he did, followed by an rm -rf *

The problem was that he typed "su -" which moved him to the root
directory. Not even a series of messages like "/bin/rm: Cannot remove,
file busy" detered him, until the machine was wiped out...

A catch for coughin'

Dave Horsfall <munnari!stcns3.stc.oz.au!dave@uunet.UU.NET>
Sat, 18 Jun 88 15:57:42 est

From "Computing Australia" 13 June 1988:

"System slip leads to danger dosage

An error in instructions given to a pharmaceutical manufacturer's computer has resulted in the production of two dangerous batches of cough mixture.

A spokesman for South Australian Hamilton Laboratories, which makes the Neo-Diophen Elixir, said during preparation of the master batch documents for the computer, a decimal placing was typed incorrectly [another decimal point error?].

Some of the mixture was found to contain 10 times the normal level of a certain chemical, he said. He said about 6,400 bottles of the mixture had left the laboratory, but less than half had reached retail outlets.

The Federal Community Services and Health Department issued an instant recall on the batches and last week department inspectors were investigating the mistake."

So it's not the cough that carries you off, but the coffin they'll carry
you off in...

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

---

Eric Roberts <roberts@decwrl.dec.com>
Mon, 13 Jun 88 15:54:26 PDT

I found this amusing, particularly in light of the fact that the

OTA has been investigating SDI software feasibility. /Eric

Congress of the United States
Office of Technology Assessment
Washington, DC 20510-8025
June 6, 1988

TO OTA'S MAILING LIST:

Thank you for your effort in filling out and returning OTA's yellow update flyer last March and April. Unfortunately, some software problems have delayed the recording of the new information. While we are in the process of diagnosing and solving the software problems, we will be using the non-updated list for sending out Report Briefs....

We anticipate having the mailing list up and running as normal in August.

Cordially,

OTA Congressional and
Public Affairs Office

Challenger Payoff?

Richard Outerbridge <csri.toronto.edu!outer@uunet>
Sun, 12 Jun 88 21:44:18 EDT

Recently I heard a litigation lawyer speak on the connection between insurance premiums and corporate motivation. He claimed that despite the shuttle disaster Morton Thiokol still received a $65 Million dollar "early completion" bonus on the contract that included the Challenger launch. Is this true? 'Twere scandalous 'twere so, but stranger (and sorrier) things have been known true.

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 10

Monday 27 June 1988

Contents

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

Four killed as Airbus crashes

Duncan Baillie <dmb%lfcs.edinburgh.ac.uk@NSS.Cs.Ucl.AC.UK>
27 Jun 1988 0953-WET (Monday)

This is how the Airbus crash in France was reported on the front page of the Guardian. Unfortunately it is rather short on facts but no doubt these will follow.

From The Guardian, June 27 1988 (copied without permission).
by Paul Webster, Michael Smith, Peter Murtagh.

At least four people were killed and at least 30 more unaccounted for last night after a European Airbus using a controversial computer controlled flying system crashed into a forest during a demonstration flight at an airshow in eastern France.

British Airways and Air France suspended further flights of the plane, the A-320 which is Europe's most advanced passenger aircraft and is built by a French, British, West German and Spanish consortium. British Airways has had two A-320s in service since the spring and orders for a further eight.

The future of the aircraft, in which British Aerospace has a 20 per cent stake worth 450 million pounds, and builds the wings and tailpiece, will be placed in doubt after yesterday afternoon's crash, the first disaster to hit the new generation of European Airbuses.

The plane, carrying 127 guests, airshow joyriders and journalists, was flying low over the small airport at Habsheim, about 10 kilometres from Mulhouse in southern Alsace when the pilot let down the undercarriage and made two passes over the local aeroclub buildings. As he turned the plane the wheels caught the tops of the pine trees and plunged into the forest.

It burst into flames shortly afterwards but many of those on board appeared to have escaped. Reports of people trapped inside could not be confirmed but the French authorities said that about 100 passenegers had been injured, two of them seriously.

A policeman among the first on the scene said "The plane did not go into a nose-dive. It belly flopped onto the trees." The pilot who had minor head injuries, told a rescuer: "I tried to accelerate but the plane did not respond."

A photographer among the passengers said the aircraft was turning when there was "a noise as if we were travelling along a bumpy road". He saw the tops of the trees and the plane caught fire near the cockpit when it came to a standstill.

He said: "There was no panic and I only saw one woman passenger who seemed seriously hurt. She was quite badly burned," he added.

The narrow bodied plane, designed for short to medium-range flight, went into service only last Thursday with Air Inter, the internal French airline, where pilots have been protesting for more than three years about its safety. In spite of warnings that the plane's two-man cockpit, without room for a flight engineer, was potentially dangerous, 21 airlines have ordered 522 of the planes.

The crash could not have come at a worse time for the Aitbus whose reputation has been built on an impressive safety record since its first model went into production 18 years ago.

The A-320 is the first civilian aircraft to use a computer-controlled flying system known as "fly-by-wire". This replaces the conventional stick and rudder control with three computers and miles of electronic cables, leaving the pilot with a "sidestick" like the control arm on a video game.

The pilot uses it to direct the computers but they direct most of the instruments. However, if the pilot makes an error or unreasonable demands on the engine, the computer can over-rule his command.

Last night Professor Bev Littlewood, of the software engineering department at the City of London University, questioned the system's safety.

He said: "We have gone so far along the rocky road of computer control, it is now hard to ask fundamental questions about critical safety areas."

Last year, the A-320 system was criticised by Mr Brian Perry, head of Avionics and Electrical Systems for the Civil Aviation Authority. He said: "It's true we are unable to establish a fully verifiable level that the A-320 software has no errors. It's not satisfactory but it's a fact of life".

An Airbus spokesman said: "Airbus planes have flown over 5 million hours. In all cases the aircraft was not to blame". There have been three crashes involving Airbuses but none had caused casualties, he said.

Laziness as an excuse

Matthew P Wiener <weemba%garnet.Berkeley.EDU@violet.berkeley.edu>
Sat, 25 Jun 88 08:38:59 pdt

This is forwarded from Robert L Park's "What's New" in the physics group, dated 24 June 88:

3. RESTRICTIONS ON ACCESS TO UNCLASSIFIED DOE TECHNICAL REPORTS came to light when the DOE's Office of Science and Technology Information offered "some limited reports" to university libraries if they would agree to grant access only to government agencies and principal investigators on DOE contracts. Most libraries refused on principle, but they wanted to know what they weren't getting. In response to a Freedom of Information request from the National Security Archive, however, DOE refused even to provide a list of titles, claiming the information was stored in a computer and thus could be retrieved only by writing a new program! The Office of Hearings and Appeals last week overruled DOE, pointing out that agencies would otherwise be allowed to conceal information simply by putting it in computerized form.

ucbvax!garnet!weemba Matthew P Wiener/Brahms Gang/Berkeley CA 94720

Privacy vs. Security

Larry Hunter <hunter-larry@YALE.ARPA>
Thu, 23 Jun 88 11:52:00 EDT

I recently applied for a job that would require a security (Q) clearance. I was handed a form for "pre-employment screening" that any job offer would be contingent upon. I was surprised by the invasiveness of the form I was being asked to sign:

"I hereby authorize the [employer] and its agents to inspect, copy or

photostat any or all documents pertaining to my financial records, my education records, my personal references, my employment records, and local law enforcement records as they pertain to me. `Documents' shall be construed in its broadest sense including any original, reproduction, or copy of any kind of written, printed, recorded, documentary material (or drafts thereof), or graphic matter regardless of the medium on which it is produced, reproduced, or stored, including, but not limited to, correspondence, memoranda, inter or intra-office communications, notes, diaries, calendars, contract documents, publications, calculations, estimates, vouchers, minutes of meetings, invoices, reports, studies, computer tapes, computer cards, photographs, negatives, slides, dictation belts, voice tapes, telegrams, notes of telephone conversations, and notes of any oral communications."

Note that there is no time limit on this authorization, and that this is merely pre-employment screening, not yet an application for a clearance.

Have all of you folks with clearances agreed to something similar? Is national security incompatible with the personal privacy of those who are aware of security matters?

Larry Hunter, hunter@yale.edu

Re-using government databases

Amos Shapir <nsc!taux01!taux01.UUCP!amos@Sun.COM>
17 Jun 88 12:13:14 GMT

The Israel Broadcasting Authority is a semi-independed agency, funded in part by a tax on radio and TV sets (called, for historical reasons, 'TV license fee'). Anyone owning a TV or renting one should inform the IBA of this fact, so they know where to send the bill. Naturally, many people evade the tax by not informing the IBA when they move.

This week, the IBA used a computerized database to send all people older than 26 and listed as living with their parents, letters informing them that the law requires that any change of address be reported to the IBA.

The assumption is that most of these people no longer live with their parents, have their own untaxed TV sets, and that their parents will forward the message. I don't know what database they have used, since I also got such a letter, but have not been living with my parents for years.

Amos Shapir

National Semiconductor (Israel), 6 Maskit st. P.O.B. 3007, Herzlia 46104, Israel Tel. +972 52 522261 amos%taux01@nsc.com

Root Bloopers

Doug Krause <dkrause@orion.cf.uci.edu>

Thu, 23 Jun 88 03:43:09 -0700

Try typing 'kill 1' when you really mean 'kill %1'.

Douglas Krause, University of California, Irvine

Problems with VARs

Hal Norman <norman@devvax.Jpl.Nasa.Gov>
Fri, 17 Jun 88 9:07:43 PDT

In response to Jerry Harper's troubles with a VAR, I have had (am currently having) a similar problem. I bought a XT clone for my home use from a "reliable" VAR. It came with a 1 year warranty. About 4 months after I bought it, it started making horrible noises. I opened it up and it was the fan on the power supply(PS) that was making the noise. I called my VAR and was told to return either the whole unit and they would replace the PS or just bring in the PS and get a new one. So I removed the PS and took it in for replacement. The owner was not there at the time and an employee exchanged it for me. I made the mistake of not getting a receipt showing the serial numbers of both power supplies (the bad one and the replacement). About a week later I got a call from the owner claiming that I had foisted a bogus PS off on him. He was quite irate, claiming he had never ever carried the brand of PS I had returned and wanted me to pay him $60 for the replacement. I copied my original receipt (with the PS serial number) and sent him a copy, but he claims it doesn't match the one I returned and still demands $60. Meanwhile, the replacement PS developed the same fan problem as the original and had to be replaced. I took it in and he replaced it, but is still irate and wants $60. I told him to send me a bill, and as soon I get the bill that I would file in small claims court and we could let the Judge sort it all out and decide how much if any I owed him. I have not yet gotten the bill. The point is, when you buy something as complex as a computer, make sure you get a receipt signed by the VAR specifying ALL the serial numbers of ALL the components and verify that the list is correct. Then, if you should have to take it back for warranty repair, make sure you get a receipt for any swapouts indicating BOTH the serial number of the new unit AND the serial number of the bad unit.

Hal Norman -
Disclaimer: These are my personal opinions and are NOT to be construed as those of my employer.

Fail-safe ATMs (RISKS-7.9)

Steve Philipson <steve@aurora.arc.nasa.gov>
Wed, 22 Jun 88 15:46:31 PDT

In RISKS 7.9 dcatla!mclek@gatech.edu (Larry E. Kollar) writes:

> The ATMs around Atlanta always give you a receipt, whether or not ...

In California, Security Pacific's ATMs (part of the STAR System) issue

a message that the machine is out of receipts, and ask if you want to proceed. You can still make transactions, but as we have seen, there is a higher degree of risk. Many ATM transactions don't generate a receipt. Account balances, for example, are displayed only on the electronic display and no receipt is given.

There is no way that receipts can cover all contingencies. A machine that will not operate if it is out of receipts reduces the magnitude of the problem, but what happens when the receipt producing mechanism fails, either by the print mechanism, feed mechanism, or receipt quantity sensor failing? A good design should try to minimize abnormal transaction termination, but it must also have provisions for unanticipated failure modes to be handled gracefully -- soft failures instead of hard failures. Audit trails sometimes get screwed up, too.

It seems that in order for all parties to get maximal protection from errors, there should be multiple independent levels of redundancy and record keeping. Independent video tapes of the customer AND display screens would provide a mechanism for resolving discrepancies, but I know of no systems that use this technique. Many ATMs look like they have cameras to monitor customer (ab)use, but often it's just a dummy camera to discourage vandalism.

Even telephone systems to report problems won't catch everything. Failed transactions may not make it clear that a problem needing correction occurred, so there would be reason to report it.

We're a long way from making automated systems foolproof. Thus we must monitor such systems and not let the service providers call all the shots.

Malicious Code Reports

"Joseph M. Beckman" <Beckman@DOCKMASTER.ARPA>
Thu, 23 Jun 88 15:40 EDT

As a member of the National Computer Security Center, I am asking for direct contributions of reports on malicious software. Please report computer viruses, trojan horses, or other forms of offensive software. I and the Center will use this information to track attacks, gain an understanding of system vulnerabilities, and develop defenses. Please send your reports to:

SOFTWARE @ DOCKMASTER.ARPA.

Joseph

P.S. If the information is proprietary or not-to-be-shared, please indicate on the report. The NCSC shares some information with NBS. I will try to release summaries or abstracts to RISKS (of the non proprietary/secret variety); although it may formally come through NBS.

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 11

Wednesday 29 June 1988

Contents

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

Risks of answering machines

Dave Horsfall <munnari!stcns3.stc.oz.au!dave@uunet.UU.NET>
Sat, 25 Jun 88 16:19:31 est

From the Sydney Morning Herald, 13 June 1988:

``Careless talk: it's a message machine

Alan wasn't at home when his girlfriend Donna called him yesterday morning. Nor could he take his father's call. Or a call from his other girlfriend, Jenny. I know this because Alan owns an answering machine just like mine. It is so similar, in fact, that my remote control unit _lets_me_listen_to_his_messages_ [emphasis mine!].

The machine in question is a Tandy, but the 'Herald' has discovered that anyone can listen to messages left on most of thre many thousands of answering machines already in people's homes. This is because most remote-control answering machines have primitive codes, and many have none at all. [... 14,000 like this sold in a three-week sale ...]

[... how the remote tone coders work - just one of four tones]

[... Tandy had sold "tens and tens of thousands" of this model - the TAD-212 - and similar machines in 2 years ...]

Dick Smith Stores [a consumer electronics chain] also sell answering machines which are activated by voice pattern. [The product manager] said the group had sold more than 20,000 such machines. By talking for a set period of time, keeping quiet for a set period of time, and then talking again, the machines can be activated. He said every machine responded to the same voice code. "You would not recommend that anybody leave vital information on an answering machine," he said.

Ms. Phillipa Smith of the Consumers' Association said the privacy and security problems associated with these machines were "quite obvious". "I think most consumers would assume there was a built-in personal-identification system," she said. "This really is an area where technology has outstipped the law."

Dave Horsfall (VK2KFU), Alcatel-STC Australia, dave@stcns3.stc.oz

---

Airline reservation crash (A new definition of "virus" ?)

Dave Horsfall <munnari!stcns3.stc.oz.au!dave@uunet.UU.NET>
Sat, 25 Jun 88 14:33:39 est

The following appeared in "Computing Australia" (affectionately known as "Confusing Australia") 20 June 1988 and appears to define a new form of virus:

``Virus shoots down flight reservations

Hundreds of travel agents in two states went offline after a virus caused a system crash. Staffs of Travel Industry Automated Systems (TIAS) last week told of their "organised panic" as the virus spread through the Multi Access Airline Reservation System (MAARS), which covers agents in New South Wales and Queensland.

TIAS technical manager Michel Radecki said the virus appeared in the form of corupted statistical data on June 9 soon after software changes. Software supplier Memorex Telex said an onsite power interruption on the night of June 8 was believed to have caused the problem. The company's manager of airline applications and support, Alan Sitters, said data was not disk-converted [?] during the interruption, resulting in incomplete information entry into the network. He said the cause was external and the MAARS software was not at fault.

Radecki said about 450 users were offline for several hours over two days as Memorex Telex trouble-shooters joined inhouse staff to fix the problem. TIAS staff had staff shut the 275-user queuing system to

> pinpoint the fault, but the virus quickly spread to the reservation system and information database, he said.
>
> [...]
>
> He said the software changes had been made about one week before the crash to test the integration of American Airlines [!] into the system. The TIAS network already had access to 35 airlines' reservation systems.''

So, a power failure causes corruption of input data, and with no apparent sanity-checking, goes on to corrupt other data. Is this a virus? If it looks like a crow, and sounds like a crow...

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

---

Update on Airbus crash

Duncan Baillie <dmb%lfcs.edinburgh.ac.uk@NSS.Cs.Ucl.AC.UK>
29 Jun 1988 0950-WET (Wednesday)

The airbus story seems to have been dropped from today's news, probably being overshadowed by the Paris Train crash (which killed 57). There were some more details yesterday, but I don't have them to hand. It seems however that the blame for the crash is being placed squarely on pilot error. Apparently the pilot had TURNED OFF the computer for the demonstration flight and was flying the aircraft at 30 feet, 70 feet below the minimum safety level. The pilot has said that he requested more power from the engines but it arrived to late (from film of the accident you can hear the power coming on just when the plane clipped the top of the trees). I believe that manslaughter proceedings may be brought against the pilot.

British Airways have stated that they are satisfied the cause of the crash was not any design fault in the aircraft and have resumed service with their own A-320s.

It is amazing that more lives were not lost in the crash as there was a large explosion a few seconds after the planes came down. The only recognizable features in the burnt out wreckage are the tailfin and part of the left wing. The planes automatic escape chutes, which opened as soon as the plane crashed, seem to have been the reason that so many people were able to leave the plane so quickly. Many people clearly have their lives to thank for this safety feature.

In accidents such as this there are usually some other contributory factors but for the moment pilot (and co-pilot) error is the main source of blame. The risks: perhaps the major risk was the lack of faith the pilot had in the computer (French pilots have been voicing concerns for some time about the aircraft's safety) so the major question is why was the computer turned off?

Re: Airbus A 320 crash - risk of `Fly by Wire'?

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

West German newsmedia began to report about possible risks of the Fly-by-wire technology of the Airbus A-320 only after a spokesman of Cockpit, an international pilots association, said that his organisation had severe doubt about the `official' version (as having been published by the responsible French minister a few hours after the accident) that the pilot made severe mistakes. In the meantime, public authorities in France, UK and Germany as well as Airbus Industries (through the chairman of the board, MP Strauss from Bavaria) interprete video-films showing the `demonstration flight' including the final phase with the following arguments:

1. `demonstration flights' aimed at demonstrating the aerodynamic limits (e.g. low height, low velocity) are only allowed without passengers, with small amount of kerosene and only with specially educated test pilots; since Mulhouse airport is only a very small airport, a demonstration flight would have never been allowed by the French authorities; the two French pilots, though Air France's most experienced Airbus pilots, were not properly educated;

2. the pilots have (against rules) switched to `manual control'; as can been seen in the videos, the plane was as low as 30 feet at a velocity of only 140 Knots; the trees shortly after the end of the runway were about 40 feet tall, but the pilots could not see the tree-tops because of the elevation of the plane's nose in the simulated landing procedure;

3. while the pilots say, that the engines didnot follow their signal `speed-up', the officials say, that this signal was given too late; assuming that the simulated approach was done under `running idle' conditions, the engines need 8-10 seconds to accelerate to max. RPM; from the moment where the engines really began to accelerate, until the moment where the plane reached at top of the first trees, only 5-6 seconds were past.

Despite the official version (which allowed the French, UK and German Airbus A-320 planes to be in the air again after 1 day of flight prohibition), several questions are un-answered:

a. Did the pilots fly under `manual control'(as the officials argue, while some experts said that such a mode doesnot exist for simulated landing)?

b. If under manual control, did the pilots fly (contrary to experienced behaviour) with the engines running idle (then needing 8-10 seconds to accelerate the engines), or did they run with `drag gas' (German: Schleppgas) after which the engines need only 2-4 seconds for maximum RPM? In both cases,

why did the engines only react on gas-giving with retardation?

(Cockpit officials say, that experienced pilots fly such manoevers with drag gas: this reaction time would have allowed to avoid the accident when all other technical conditions are in good orfer; they trust their colleagues statement that the engines didnot react instantaneously, and they continue to speek of a technical problem)

c. Was the demonstration flight authorized? The Airbus was transferred to Air France only 2 days before, and evidently this was its public maiden flight.

The very fast reaction of government and industry is not surprising: Airbus Industries hopes to build and sell more than 500 Airbus A-320 models in the next 10 years. Though the governments of France, UK and FRG are responsible for airtraffic safety, they have also invested more than 10 Billion Dollars into the diverse models, and they are interested in minimizing the risks from prize guarantees which they have overtaken also for A-320. It seems rather doubtful whether guaranteed security was the reason that the responsible French minister excluded any technical risk before technical investigations could have given enough evidence.

Though severe problems with computerized equipment in military aircraft have recently drawn public interest to safety in airtraffic, the A-320 accident for the first time draws public attention to risks of overreliance on computers. Officials as well as technicians argue that the technical system is much safer than any other plane before or even today; if there is any risk, than it is `only the risk of the human operators'. If you leave the `holistic approach' aside (according to which the security of a system consisting of humans and machine is not greater than the least secure component), there remain also design considerations to be analysed:

If a pilot cannot see, in the typical approach configuration `nose up', the ground several 100 meters before his nose, is it responsible to have a `manual landing mode' at all? (In this case, the demonstration of slow, low flight would have been impossible, but also no victims!)

As pilots control involves human errors, automatic control also involves human decisions, namely those of designers and programmers; even if they were flight experts, they cannot foresee (not only in todays limitations, gut generally) all situations of the `real application situation'. A totally computerized system like the A-320 where no mechanical aid helps to correct electronic shortcomings is by its very design principles less adaptible to unforeseen real world events.

Unfortunately, it is not so unprobable that several more accidents may falsify the official optimism which describes this plane as `the most secure plane ever built'; but fortunately, public media

begin (at least in FRG) to wake up from such dreams.

Klaus Brunnstein Univ.Hamburg FRG

---

re: Four killed as Airbus crashes [Actually Three?]

<Laura_Halliday@mtsg.ubc.ca>
Mon, 27 Jun 88 09:48:58 PDT

In an interview on the BBC World Service this morning, an aviation expert commented that some pilot errors cannot be easily remedied by computer. In particular, once the landing gear is down, the on-board computers assume that the pilot intends to fly the plane down to ground level, otherwise the A320 could not land until it ran out of fuel.

This implies the existence of elaborate lockouts - what if the pilot intends to make a wheels-up landing (for whatever reason)?

Laura Halliday laura_halliday@mtsg.ubc.ca

---

root typos (could happen to anyone)

Joe Eykholt <jre@Sun.COM>
Tue, 28 Jun 88 17:38:51 PDT

How about "rm *>o" instead of "rm *.o" this can be caused on many keyboards by holding the shift key down a little bit too long.

Don Sterk at Amdahl pointed this one out to me, after it happened to him once. The shell creates the file "o" then rm removes it and everything else.

Joe Eykholt

"large-scale" disasters (Hinsdale, Ill.)

Tom Perrine <hamachi!tots!helix!tep@nosc.mil>
Tue, 28 Jun 88 14:16:18 PDT

A few questions and comments about disaster planning and the recent Illinois Bell central-office (C)) fire in Hinsdale Ill.

This seems to be the first time that such a relatively small fire has destroyed so much communications capability. The Hinsdale CO was apparently carrying most (if not all) of the communications traffic for lots of large, information-intensive businesses.
***Is this CO typical of others around the country?

Many (or most) of the companies involved had placed the probability of interruption of the carrier's service as fairly low.

***Is this typical of companies that depend on communications common-carriers?

According to interviews in "Network World," many of the network managers of the affected companies were "shocked" at the lack of a fire-control system. This has led to threats of litigation.
*** Any comments?

Even though this was a communications failure, and no customer's equipment was damaged, several companies were forced into their full-scale disaster plans, because they either had not addressed loss of communications separately or these "mini-disaster-plans" were not workable (e.g. the backup phone lines also went through the same CO). This is *much* more expensive than just restoring communications would have been (United Stationers, Inc. spent nearly $600,000 to move to its backup data center).
*** How many companies would be in the same situation if this happened to them?

Has anyone (or any organization) announced plans to try to conduct a large-scale multi-company post-mortem examination of the incident? This would appear to be a golden opportunity to examine a wide range of disaster plans, produced by many different organizations and determine which features of each plan were most or least useful. This could lead to better overall disaster planning for the industry as a whole.

Tom Perrine hamachi!tots!tep@NOSC.MIL (last resort:Perrine@DOCKMASTER.ARPA)
Logicon(Tactical and Training Systems Division) San Diego CA (619) 455-1330

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 12

Thursday 30 June 1988

Contents

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

Airbus 320 (RISKS-7.11)

Steve Philipson <steve@aurora.arc.nasa.gov>
Thu, 30 Jun 88 13:18:20 PDT

Here are some comments on the A-320 crash, official reports, and unofficial speculation.

It is truly amazing that official sources attributed the accident to pilot error virtually before the investigation began. A decision seems to have been made to protect Airbus and blame the flight crew no matter what the facts. It was grossly irresponsible to exonerate the aircraft before the flight data recorders were examined, or experts had time to analyse the video tapes and other data.

There are several questions that many people have not asked that are critical to an understanding of this accident. If the aircraft was indeed only at 30 feet of altitude, why was it that low? Did the pilot intend to descend to that height? What was the minimum altitude authorized

for the low pass? What was the actual airspeed, the pilot-commanded/desired airspeed, and the minimum authorized airspeed?

Observers claimed that they heard the engines spool-up too late. The conclusion is that the pilots did not allow for the spool-up delay. Such a delay is NOT specific to the A-320 but is rather a characteristic of all turbo-jet engines. Why would an experienced crew have delayed adding power, or even throttle back to low idle, when a high-speed idle would have made engine response much quicker. When did the crew command a power-increase? Was it several seconds BEFORE witnesses heard the engines START to spool-up?

Some maintain that the "computer was turned off". This is an interesting concept for an aircraft that flies completely by electronic controls. There are no direct manual controls of the primary flight surfaces or engine controls. Some auto-matic features may have been de-selected. It is of great interest which these were and how the selected systems operated.

> The planes automatic escape chutes, which opened as soon as the plane crashed,

That's an interesting report. As far as I know, there is no automatic door opening / escape slide deployment mechanism. Slides inflate auto-matically once doors are opened manually. The likely reason that so few lives were lost is that the aircraft contacted the trees in wings level, controlled flight, with the nose up. The lower fuselage structure and wings absorbed much of the impact, and as trees were destroyed they relatively gradually slowed the aircraft.

> I believe that manslaughter proceedings may be brought against the pilot.

What will be the outcome if we find that an aircraft system was at fault? Do we bring charges against Airbus management, engineers, or software programmers?

It is interesting that British Airways is satisfied that the aircraft was not at fault. How could they have made that decision before any data on the accident was released? Every day that their airplanes sit on the ground costs a lot of money in lost revenue, and is negative publicity for their shinny new airplanes. The airlines thus have a proprietary interest in keeping them flying.

Officials blame a flight crew that was chosen for its experience and abilities. This crew was extensively trained and passed certification exams on systems and flight of this aircraft. That such a crew could be involved in an accident like this indicates that the aircraft is not immune to accidents, even with it's advanced technology.

The A-320 may have been designed to be more safe than older technology craft, but this does not mean that it is. Only operational experience will establish the actual risk. A major concern of systems analysts and pilots is that automated systems may actually increase risk as the pilot is not "in the loop", at the least not to the extent he is in other aircraft. Operational experience has shown us that automation introduces new problems as it addresses some old ones. As of yet, we have no data

to show that the highly automated A-320 will be as safe, less safe, or more safe than older aircraft. We may learn a lot about the aircraft from an analysis of this accident. We will certainly not know why the accident occurred or if anyone is to blame until the investigation is complete.

Steve Philipson

Background on the A-320 incident

<willis@rand-unix.ARPA>
Thu, 30 Jun 88 10:14:10 PDT

Given the extensive commenting on the A-320, perhaps these observations will be useful. They're based on my personal knowledge of avionics as it is implemented and practiced in USAF aircraft and in the 757/767.

Incidentally Klaus Brunstein quotes the investment in the A-320 as $10 Billion. I wonder whose "billion" he's using; if it's the English billion, that's an investment of $ 10*13 -- lotsa bucks.

The USAF F-16 tactical fighter is a fly-by-wire and implements flight control with a quad-redundant analog (YES - analog) computer in the belly of the plane. It is a microcircuit analog implementation to be sure, but nonetheless avoids the software problem in flight control. There are no cables from the cockpit to the control surfaces except for trim tabs. If the quad-redundant machines are lost, the pilot can try to land the plane by manipulating trim tabs. Needless to say, one of the earliest changes to the aircraft was to put protective armor around the flight controllers.

There is a separate 65K (as I recall) computer that integrates aircraft functions, delivers signals to the flight control analog system, receives signals from it, talks to the software-controlled heads-up-display, receives digital inputs from the inertial navigator and from manual pilot inputs, manages the radios, receives signals from and sends control signals to the software-controlled radar, transmits pilot inputs to the digital weapons-control subsystem and receives status information from it, receives and logs all fault indications from the entire aircraft and runs diagnostic tests on itself and on other subsystems, AND manages cockpit instrumentation and display. The sytem also monitors for some danger conditions, e.g., wheels up but ground clearance approaching zero. Everything communicates with everything else on a 1 Megabit/sec digital redundant MUX bus.

As I recall, pilot intentions (originating by a non-moving pressure-senstive side stick) are communicated directly to the flight control system which then relays them to the digital systems. Thus the pilot could fly the airplane IF the master digital system failed, although he might have no instrumentation (at one time there was a debate about leaving a few "round instruments" in the cockpit as fallback).

USAF has experimented with and test flown a digital fly-by-wire system, but I don't know whether it's been implemented in more recent aircraft, or

even in the upgraded F-16. Odds are that newer fighters (e.g., F-18s and F-20s) are all-digital. Almost surely the ATF will be all-digital.

Even though the analog system actually flys the F-16, it gets inputs and control from the digital systems. In particular, the acclerometers of the inertial nav system report dynamic acceleration and if it's too high, the intent of the pilot is overriden by the software controls to avoid tearing the wings off the plane and blacking out the pilot. In fact pilots have complained about this because they would be willing to risk aircraft damage and/or blackout to escape a pursuer or perform some maneuver.

In US commercial aircraft that have "glass cockpits" (as the CRT displays are called), flight control has continued to be traditional direct cable linkage for the most part although hydraulic boost is almost always needed. There are aircraft in which the stick motions control only a hydraulic system which is the only linkage to the surfaces.

There usually is an all-digital system called by some such name as "Flight Director" that does or helps with navigation (especially on inertial-nav equipped aircraft), controls the aircraft trajectory in conjunction with an autopilot or other nav inputs, might support fuel management, might handle the aircraft through Cat III (blind-landing) procedures, controls the descent from flight altitude to minimize fuel consumption, handles the throttles to conserve fuel consumption, etc.

Without a lot of technical details, one cannot know how the A-320 designers implemented their software and distributed the functionality across one or more computers. Odds are that the flight control is in a separate and redundant set of machines for safety. If the designers were astute, the redundant machines are powered from separate power sources and through individual circuit breakers. [There is a recorded instance in a commercial aircraft of the pilot losing an important instrument because it was powered through a circuit breaker that also happened to control some inconsequential other thing -- such as lighting.]

So any comment about "shutting off the computer" (in the A-320) must refer to the flight management system, not to flight control. Airlines are forever interested in optimizing cost of operation, and who knows what flight-profile or flight-maneuvers may have been incorporated into the A-320 systems? Who knows what combination of danger situations have been programmed in -- and the flight crew blundered into? Who knows whether the aerodynamically possible and economically desired flight envelope has been built into the software -- and the flight crew accidentally violated?

One can easily imagine a software requirement that says something like:

```
IF   engines throttled back AND wheels down AND altitude less
 than ..... AND rate of descent equal to .... AND speed less
 than .....

THEN aircraft is landing and adjust angle of attack to .....;
 also check for proper fuel-flow conditions for landing, check
 flap position, ......
```

In spite of what has been said, I personally am not yet ready to conclude that a software anomaly lurks in the A-320. Personal opinion of course, but it sounds suspicious to me.

There is one other observation about glass cockpits that my friends in the business have told me. Round instruments not only indicate some parameter but they also convey rate-of-change information. Glass instruments evidently have been implemented to convey only the parameter value, not the derivative of the parameter. If true, one can imagine that in some circumstances the flight crew is denied helpful and possibly critical information about events.

Willis Ware

Fly-By-Wire

"John O. Rutemiller" <Rutemiller@DOCKMASTER.ARPA>
Thu, 30 Jun 88 09:12 EDT

When considering the safety of a fly-by-wire system compared to a "normal" system, you must consider whether the overall safety of the system is improved. Granted there are failure modes in fly-by-wire that would not otherwise exist, but there are also a lot of things you can do with fly-by-wire that you would not be able to do with a "normal" system. If the overall safety of the system is improved, then it is a better system.

[But don't forget that if the aircraft is designed to be aerodynamically unstable (i.e., without the computer) -- as are some high-performance planes -- overall safety can be nonexistent under certain conditions. At the IEEE COMPASS '88 this week, John Cullyer noted that in a fully fly-by-wire plane such as the planned Eurofighter, the pilot will have at most two seconds in which to decide whether to eject, after which it may generally be too late. (The Experimental Aircraft Project is developing a plane that will be -12% (un)stable. John described the VIPER effort, which is being subjected to extensive formal proofs, and which is being designed for the EAP.) PGN]

Airbus 320 (Re: RISKS-7.10)

"H.Ludwig Hausen +49-2241142426" <HAUSEN%DBNGMD21.BITNET@CUNYVM.CUNY.EDU>
Thu, 30 Jun 88 09:54

There was a video on German TV Newsshows (ARD, ZDF, SAT1) indicating that the Airbus plane
1. was 10 meters above the ground
2. in a position making the pilot unable to see the trees at the end of the runway (which was too short for landing an Airbus)
3. engines got power far to late to get back into secure hights.

Seeing the video one will get the impression that the whole thing

(going to a small, badly equipped airfield and doing demonstrations) was a very risky PR manoeuver. There might be some serious problems with this Airbus plane (see B. Littlewoods comments) but I guess this time it was the pilot's fault. H.L. Hausen

$40 million Pentagon computer system failure

Rodney Hoffman <Hoffman.es@Xerox.COM>
30 Jun 88 07:45:04 PDT (Thursday)

From the Los Angeles Times, June 29, 1988:

PENTAGON COMPUTER SYSTEM CALLED A $40-MILLION FAILURE

The Pentagon's latest effort to unscramble its tangled foreign military sales accounts has been a $40-million failure, the House Government Operations Committee said Tuesday. It said a costly new computer system for straightening out the botched program was two years behind schedule, had thousands of unresolved problems and ultimately could cost $75 million without performing well.

As a result, the committee said, the Defense Department cannot say why there is an unreconciled $1-billion difference between cash on hand in a special trust fund and total payments by foreign countries that purchase U.S. military equipment through the foreign military sales program. "The [foreign military sales] trust fund system is in shambles," Committee Chairman Jack Brooks (D-Tex.) said....

The new accounting system, developed by the SAGE firm of Rockville, Md., for the military, was supposed to be ready in October, 1986. Now the completion date has been postponed until next October, or two years behind schedule.

Re: Another "silent fault tolerance" example: DWIM

Mark Brader <msb@sq.com>
Mon, 27 Jun 88 16:11:44 EDT

Path: sq!utfyzx!utgpu!utzoo!attcan!uunet!husc6!bloom-beacon!tut.cis.ohio-state.edu!rutgers!orstcs!mist!budd
From: budd@mist.cs.orst.edu (Tim Budd)
Newsgroups: comp.lang.misc
Subject: Re: What makes a language "easy" to program in?
Date: 17 Jun 88 20:31:42 GMT
Organization: Oregon State Universtiy - CS - Corvallis, Oregon

No, I'm not sure you want a ``do what I want'' command.

The following story is true, I've just forgotten some of the less important details. There was a Lisp system once that had something called DWIM (do what I mean). If you typed an expression, if it didn't make sense, it would try various techniques to see if something close to it made sense, and do that. Now a friend of mine was using this system and kept having amazingly

slow programs. It turned out he was saying things like (CAR ...) when the system wanted (car ...). It would not recognize CAR, go through some analyzing, discover that a probable meaning was car, then do it. Problem was there was no feedback - no indication he was doing anything wrong, it produced the right answer, just slowly. So there are dangers in ``do what I want'' systems even when (and this is a big if) they can exactly figure out what it is that you want.

[Forwarded to Risks by Mark Brader]

[That was Warren Teitelman's INTERLISP environment. PGN]

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 13

Friday 1 July 1988

Contents

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

"Scratch-and-win"? Try "X-ray-and-win"!

Peter G. Neumann <NEUMANN@csl.sri.com>
Fri 1 Jul 88 07:53:07-PDT

The Ontario Lottery Corp in Canada has removed all Money Match and Double Dollar tickets from sales (about $8M Canadian [per week?]) because tests have shown that the numbers under the latex patches on the $2 tickets could be read with 100% accuracy using x-ray equipment -- albeit at some expense. Lottery Corp's president Norman Morris said, "There's always somebody working to beat the system, and we're constantly working against them to improve the system." He added that the withdrawn tickets were much better than those made five or

six years ago [but still not good enough!]. [Source: The Globe and Mail, 15 June 1988, front page article by Mary Gooderham]

This is another example of the continual escalation resulting from more sophisticated attacks responding to more sophisticated technology. Past RISKS cases have included microprocessor-controlled slot machines, computer system breakins, internal frauds, and of course -- over many years -- phone phreaking.

SDIO computers stolen [old story not previously noted here]

Peter G. Neumann <NEUMANN@csl.sri.com>
Fri 1 Jul 88 07:32:02-PDT

Two computers were stolen from the Pentagon's Strategic Defense Initiative Office on consecutive nights (9 and 10 April 1988). The thieves entered by sabotaging the (physical) security system. "Videotape cameras did not record the theft because they had not been loaded," according to TV station WJLA. "The station, attributing its information to unidentified Pentagon investigators, said this lapse was a common one at the agency's offices." [Source: AP, Washington DC, 24 June, in NY Times, 26 June 1988, p. 18, on the same page with "Bishops Raise Morality Issue on `Star Wars'"...]

> [One wonders whether the motive was theft of stored information, or merely theft of the equipment for its own sake!]

Did DWIM DWYW (Do what you wanted)?

Stephen D. Crocker <crocker@tis-w.arpa>
Thu, 30 Jun 88 21:10:57 PDT

In RISKS-7.12, Tim Budd relays a story about the Do What I Mean (DWIM) facility in Interlisp. For example, if "CAR" was misspelled "car", the Interlisp interpreter would trap to the DWIM facility, which would notice a probable case error, make a replacement and proceed. This facility took a lot of time if it was called repeatedly. Budd says the DWIM facility did not say what it was doing, so the poor user did not know why his program was running so slowly.

The true story about DWIM is more complex. MANY others, including, of course, the designer Warren Teitelman, can comment usefully on DWIM. Let me outline a few of the important points.

o DWIM was a collection of facilities, some intended to fix errors and some intended to facilitate programming. Various forms of spelling correction were included, as were numerous other useful error correctors. Each of these facilities could be turned on or off, and various levels of feedback were possible. It was certainly possible to disable all DWIM facilities, and it was certainly possible to insist that the user be notified and/or queried before making any corrections.

o DWIM was fundamentally an experimental system that enjoyed quite extensive use. No strong claims were made that DWIM was fail-safe, although it was

well thought out and as solid as any production code I've ever dealt with.

o DWIM was COMPLETELY documented. A relatively large fraction of the daunting Interlisp manual was devoted to the DWIM system.

Some risks are endemic in any such system:

o If a new user is given access to Interlisp with DWIM enabled, he may not know how it will operate or what it will do for him. It was not uncommon for a novice user to be set up with an environment that reflected the preferences and KNOWLEDGE of an experienced user.

o The amount of documentation was daunting. Very few users could absorb the documentation at first exposure.

o DWIM relied on various models of probable errors. Case errors are easy to understand, but some others were more subtle. DWIM would attempt to correct parenthesization errors by checking for stray 9's and 0's. If DWIM's model of probable errors did not match the user's actual error pattern, the results would range from wasting time to miscorrection.

DWIM stimulated strong feelings, both pro and con, in the Lisp community. As might be guessed, I liked it a lot, particularly because it represented the most complete collection of ideas on program error detection and correction and hence was a living laboratory. People who attempted to do research in this area and who did not have exposure to Interlisp had no idea what they were missing, and I saw some number of PhD dissertations completely wasted on poor imitations. What I never saw, however, was a serious study of how to introduce such facilities to new users and control the facilities in a way that would minimize the risks.

Directions and Implications of Advanced Computing - DIAC-88

Douglas Schuler <bcsaic!douglas@june.cs.washington.edu>
30 Jun 88 18:48:08 GMT

DIRECTIONS AND IMPLICATIONS OF ADVANCED COMPUTING

DIAC-88 Twin Cities, Minnesota August 21, 1988

Earle Browne Continuing Education Center, University of Minnesota

Computing technology in public and private institutions poses challenging technical, political, and social dilemmas. Programmers, analysts, students, and professors will face these dilemmas, either actively or unwittingly. Both within the computing profession and in the relation of our profession to other institutions, we have much to consider.

The second annual symposium on Directions and Implications of Advanced Computing will be held at the University of Minnesota campus on Sunday August 21, 1988, the day before the American Association for Artificial Intelligence (AAAI) conference.

Douglas Engelbart, the DIAC-88 plenary speaker, will share his perspective on using the computer to address global problems. Since the late 1950's, Engelbart has worked with systems that augment the human intellect including his NLS/Augment system, a hypertext system that pioneered "windows" and a "mouse." The driving force behind Engelbart's professional career has been his recognition of social impacts of computing technology. The plenary session will be followed by presentations of research papers and a panel discussion. The panel, John Ladd (Brown University), Deborah Johnson (Rens-salaer Polytechnic), Claire McInerney (College of St. Catherine) and Glenda Eoyang (Excel Instruction) will address the question, "How Should Ethical Values be Imparted and Sustained in the Computing Community?"

Presented Papers

Computer Literacy: A Study of Primary and Secondary Schools, Ronni Rosenberg

Dependence Upon Expert Systems: The Dangers of the Computer as an Intellectual Crutch, Jo Ann Oravec

Computerized Voting, Eric Nilsson

Computerization and Women's Knowledge, Lucy Suchman and Brigitte Jordan

Some Prospects for Computer Aided Negotiation, Douglas Schuler

Computer Accessibility for Disabled Workers: It's the Law (invited paper) Richard E. Ladner

Send symposium registration to: DIAC-88, CPSR/Los Angeles, P.O. Box 66038 Los Angeles, CA 90066-0038. Enclose check payable to CPSR/DIAC-88 with registration. For additional information, call David Pogoff, 612-933-6431.

NAME _____
ADDRESS _____
_____
_____
Phone (home) _____ (work) _____

Please check one:
Symposium Registration Regular O $50
(Includes Proceedings and Lunch) CPSR Member O $35
Student/Low Income O $25

I cannot attend, but want the symposium proceedings O $15

There will a reception following the symposium. Proceedings will be distributed to registrants at the symposium. Non-attendees will receive proceedings by October 15, 1988.

** MY VIEWS MAY NOT BE IDENTICAL TO THOSE OF THE BOEING COMPANY **
Doug Schuler (206) 865-3226
[allegra,ihnp4,decvax]uw-beaver!uw-june!bcsaic!douglas douglas@boeing.com

Grocery Store Barcodes: Another game you don't win

David A. Pearlman <dap@cgl.ucsf.EDU>
Mon, 27 Jun 88 17:01:28 PDT

All this talk about how ATM's don't make mistakes in the customer's favor reminds me of one of my pet peeves: When the price on the food shelf is not the same as the price scanned at the cash register.

It seems I run into this problem at least once a month at Safeway (and I've had this problem every *week* for the last month). When I catch it, the store will correct the mistake for me, but they don't offer any other sort of fix (no additional discount; no free goods). What this means is that a lot of people (who don't pay any attention) get ripped off. Those, like me, who pay attention, get the goods at the shelf price. Quite a good deal for the store, I'd say.

David A. (DAP) Pearlman BITNET: dap@ucsfcgl.BITNET UUCP: ucbvax!ucsfcgl!dap

ATM "receipts"

Mark Brader <msb@sq.com>
Mon, 27 Jun 88 10:13:29 EDT

> From: dcatla!mclek@gatech.edu (Larry E. Kollar)
> The ATMs around Atlanta always give you a receipt, whether or not your
> request went through.

I'd be very surprised if there are any ATMs anywhere that give a *receipt* for a deposit transaction. The ones I use are careful to refer to it as a *transaction record*. The distinction, of course, is that a receipt would constitute an agreement that you actually deposited the amount you claimed.

For a withdrawal transaction, "receipt" doesn't even make sense. *You* would have to give *them* a receipt, if anybody did.

Despite the above, I have in earlier days seen ATMs that referred to their transaction records as receipts. I suspect the original messages were written by programmers and not bankers...

Mark Brader, Toronto utzoo!sq!msb, msb@sq.com

Re: Risks of bank ATM cards

<dan@WILMA.BBN.COM>
Mon, 27 Jun 88 23:34:47 -0400

>From: dcatla!mclek@gatech.edu (Larry E. Kollar) [...]

>As for the printer breaking or running out of paper, it's not a hard thing
>for an ATM to detect the lack of paper flow and put itself out of service.
>Whether or not ATMs do that is yet another question.

At least some of them do. The ATMs I use (BayBanks, in Massachusetts) can tell you as soon as you begin using them if they are out of paper and cannot print a receipt; they then ask if you still want to use them. (They unfortunately can't tell when their ribbon renders the receipt almost unreadable. Oh well.) They also tell you about cancelled transactions.

Someone else mentioned the phones near BayBanks machines. I was extremely grateful for that phone a couple of weeks ago, the night before I was leaving on a trip. I had inserted my card, told the ATM I wanted $250 cash, and listened to the mechanism start whirring when it suddenly went catatonic. The display was still lit, but there were no sounds or any other sign of activity. Pressing CANCEL did nothing. It still had my card hostage, so I couldn't just go to another machine. Also, I was worried about the possibility that it had actually dished out some money in the still-locked cash drawer which might end up going to the next person to use the machine. I picked up the phone and spoke to a woman who told me, after a moment, that the teller's communication line to the mainframe didn't seem to be working. She did something and my card popped out. (I guess there was more than one line from the ATM to the great world outside.) She told me to try another machine, but not too close, as it might be using the same line. I suggested a possible other machine and she confirmed that it was on a different line; I went there and got my money. I have no idea what I would have done without the phone.

From the stories of other people, it sounds like BayBanks may do a better job than some other banks with their ATMs.

Dan Franklin

Risks of ATMs and the people who unload them

Rob Austein <SRA@XX.LCS.MIT.EDU>
Tue, 28 Jun 1988 13:18 EDT

Here's another ATM horror story. It's really a people horror story, the ATM just made things more interesting.

I have both my checking account and my MasterCard at a bank with a bad reputation for customer service but an extensive network of ATMs, which is usually ok because I use ATMs every week and talk to human tellers maybe twice a year. Last fall I had occasion to attempt to use an ATM to make a prepayment to my MasterCard from a travel advance via my checking account, because I knew that the upcoming trip would exceed my credit limit. To make a long story short, I'd forgotten whether the MasterCard had a password (PIN) associated with it, never having used it in an ATM before, so I followed what turned out to be bad instructions from the person who answered the 24-hour customer service phone, to wit, I used my normal ATM card to start the ATM session, then punched all the right buttons for a credit card deposit (which were distinct from any normal kind of deposit) and gave the machine the money in an envelope that clearly indicated that this was a payment to credit card #x. Then off I

went to California.

When I got to California and checked into the hotel, the hotel clerk told me that my MasterCard wouldn't take the estimated charge, so I made temporary arrangements and called the bank. The bank said that the fine print gave them to right to still be sitting on the payment, but that this right would expire before the day I was planning on checking out, so if I just sat tight everything would be fine. As the reader has no doubt guessed, things were not fine at checkout time, the MasterCard still wouldn't take the charge. I called the bank again and this time they had no record whatsoever of the payment, but neither were they willing to take steps over the phone such that the check would not be deposited if it were found (not in time to be useful to me, anyway). So here I was, on the other side of the country, I couldn't use the MasterCard because the bank had lost the payment, and I couldn't write the hotel a check because the bank might FIND the payment. Fortunately I also had an American Express Card for just such emergencies, so I was able to square things with the hotel and fly home to yell at the bank.

When the dust settled, here's what they told me. It seems it doesn't matter what buttons you push on the ATM if you put the wrong card in, the human who unloads the ATM processes it "appropriately" for the card you used. I.e., the effect was as if I'd deposited a check into the checking account it was drawn on. Since this is obviously a nonsense transaction, it isn't recorded anywhere (amazing logic), and I would have eventually found out what had happened when I received the UNCANCELLED check with my monthly statement and called up the bank to ask what the hieroglyphics meant.

Now, I don't know if the ATM is simply asking for more information than it's giving to the teller who unloads it in the morning (probably, I know that these ATMs only look at the first four digits of a PIN no matter what you type) or if this was an amazingly stupid teller. Maybe both. I did take the bank to task for not having at least kept track of what the ATM/teller pair had done, at which point they said that they'd had this problem before. They had also had the problem of the customer service people giving bad instructions on the phone in this situation before.

The bank did make good on all the little expenses (except time) that I had incurred during this fiasco. I think they were embarrassed about the American Express Card....

--Rob

More problems with VARs

jcmorris@mitre.arpa <Joe Morris>
Mon, 27 Jun 88 16:59:48 EDT

In RISKS-7.10 Hal Norman of JPL commented on problems of a VAR who claims that the power supply he (Hal) is trying to return as defective wasn't part of the system the VAR sold. There's a flip side to this: soon after the first customer ship of the original IBM PC, several dealers were found to be playing a game with the customers by buying a stripped PC (16K, no disk drives) and installing their own memory chips and some el cheapo disks.

They would then sell the unit at the IBM list price, making much more than if they had paid IBM's dealer price for the unit. IBM was burned repeatedly by units that failed and were returned for warranty repair; the customers thought they had bought an IBM box and weren't happy when IBM declined to give warranty service to non-IBM parts.

That's why the disk drive front panels suddenly acquired the IBM logo, so that the non-IBM drives could be more easily identified.

I don't know why the AT's (and probably PS/2's) don't sport the IBM logo. It may be that the drives themselves have the IBM part numbers or whatever on the chassis so that they can be identified; the drives on the older units have no IBM markings I can find.

Something to do on a rainy day: look at the ads in _Computer_Shopper_ and try to guess the pedigree of the major subassemblies used in some of the more aggressively-marketed clones. The number of vendors who supply that data is depressingly small.

Re: Hard-disk risks from vendors (RISKS-7.8)

George Pajari <pajari%grads.cs.ubc.ca@RELAY.CS.NET>
Fri, 17 Jun 88 14:06:19 PDT

>From: Jerry Harper <mcvax!euroies!jharper@uunet.UU.NET>
>Subject: Hard-disk risks from vendors
>We use a number of 286 machines (American Research Corporation -made in Taiwan)
> ...[details of various hardware problems]...
> ... he said he was too "busy" to come out ...[more problems]...
> ...[never] did the vendor admit any liability, nor did
> he seriously offer a replacement. This is of some concern to a number of
> Are too many people getting into the VAR market by the seat of their pants?

I get very upset with comments such as the above.

Why do consumers in the computer market (especially PCs and other low-end systems) assume that they can get more than they pay for?

Jerry as much as admits that they bought a cheap Asian clone to save money then seems not to understand why the support is non-existent?

Unfortunately your hardware supplier has to eat also and the narrow margin on his sales doesn't permit much support. Why does he charge so little? Because if he included enough mark-up to pay for reasonable support people like Jerry would buy from someone else! So it is the market (of which Jerry is a part) which supports and even encourages such vendors.

Don't complain about support unless you are willing to pay for it.

George Pajari sometime grad-student and full-time consultant
(no...I don't sell hardware...just get frustrated with clients who expect the same level of service from low-margin clone vendors as from

full-price outlets)
These opinions are those of my company. I own it, dammit.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 14

Friday 1 July 1988

Contents

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

The Eyes Have It

Woody <<WWEAVER%DREW.BITNET@CUNYVM.CUNY.EDU<>
Fri, 1 Jul 88 13:50 EDT

From _The_Star_Ledger_, Thursday, June 30, 1988 page 35, a New Jersey paper published in Newark.

THE EYES HAVE IT

MV acts to 'separate' drivers with the same name, birth date

At least 14,000 New Jersey motorists share the same names, birth dates, and eye colors, the Division of Motor Vehicles has discovered in its efforts to straighten out its licensing records.

The DMV will be sending out letters to the motorists next week asking them once again to reveal their true eye color. The agency was forced to delete the information from its computer system and use a substitute code number in order to avoid issuing the same drivers's license number ot different mororists, DMV Director Glenn Paulsen said yesterday.

When issuing driver's licenses, the DMV computer system assigns a number consisting of a letter followed by 14 digits. The letter and first nine digits represent the driver's name, the next four digits reflect the month and year of birth and the final digits is a code representing eye color.

In 14,000 cases, the DMV discovered, different motorists shared the same names, birth dates, and eye colors and had to be issued special driver's license numbers that substituted the number 7, 8, or 9 for the digits used to represent eye color.

"This effectively altered the driver license number to overcome any possible duplication with an already existing number," Paulsen said. "However, it also eliminated the individual's true eye color from the record."

Paulsen said the system has been reprogrammed so that driver's license numbers can be altered to avoid duplication, but still retain information regarding eye color. In addition, the DMV plans to change the format of its driver's license documents later this year to include the eye color information on the face of the license.

The numbers 7, 8, or 9 will still be used on licenses in place of the eye color code numbers in cases of potential duplication, but the eye color information will remain on file in the DMV's records, under the new system.

The eye color code numbers are 1 for black, 2 for brown, 3 for grey, 4 for blue, 5 for hazel, and 6 for green.

[In light of all of the stories we have had in the past involving name confusion and overzealous computer matching, this one is an attempt to do things a little more sanely -- at least to recognize the problem. But it does not seem likely that, with 14,000 data collisions, the codes 7, 8, and 9 are adequate to disambiguate on into the future, especially if new collisions arise. How about using "9" as an escape for "other" and then tack on a unique disambiguator including color. What about albinos? People with non-matching eyes? glass-eyes? tinted contacts? Lots of risks in computer matching here... PGN]

New UK Virus

Will Martin -- AMXAL-RI <wmartin@ALMSA-1.ARPA>
Fri, 1 Jul 88 10:36:42 CDT

The following is a complete item from the FEDERAL BYTES column (p. 42) of the June 27, 1988, issue of Federal Computer Week, which just arrived in today's mail (July 1):

Oh, No - Not Maggy!

Sources of reasonable reliability within the British Ministry of Defense (MoD) report that a computer virus has broken out. It seems that MoD uses a number of Macs, largely for graphics but some of them for word processing.

Whenever anyone writes "Margaret Thatcher" or "prime minister", the screen [image] vanishes, along with whatever was on it. In the place of the missing document appears a picture of Maggy, with a Union Jack behind her.

MoD, say our sources, has not found a cure.

Australia Card - more details

Chris Maltby <munnari!softway.oz.au!chris@uunet.UU.NET>
16 Jun 88 20:02:07 +1000 (Thu)

The Australia Card was not planned to be anything in particular. The design was still in the tendering stage when the whole project was canned due to a legislative technicality. Strictly speaking, the government was given a mandate by means of a dissolution and new election of both the Senate and the House of Reps which is possible only when the Senate is viewed to be obstructing legislation. The obstructed legislation was the Australia Card bill. For those unclear about the Australian Parliamentary system, the government is formed by the party which controls the House of Reps. The Senate has been/is and is likely to remain without any absolute majorities. When the new parliament was convened, a joint sitting of both houses was held to pass the bill, and it may even have been gazetted into real law, when it was discovered by a clever person that a regulation bill was required to activate the Card. The Senate indicated it wouldn't be passed so rather than face another election (and a certain loss) the Australia Card was dumped. It's ready to go, just waiting...

Suggestions or requirements for the card itself were:

> A digitised image of the person possibly on the card itself or accessible to the counter operator when the card was scanned.
>
> A digitised signature (or thumbprint) and a digitising pad which could validate the user on presentation.
>
> The card was supposed to be made from secure materials and with secure printing etc etc.

No-one had really resolved how forgery was to be prevented. An accomplice behind the registration desk would have laid the whole system open. How many forged cards would you like sir...

Now we are to have an "upgraded tax-file-number" (unspecified) if the Government can get it through the Senate. Of course, the next election will be in early 1990 so they'll have to hurry...

Meanwhile, the tax commissioner and the courts have started to interpret tax law much more strictly, and cuts in the rates have probably done as much as the card would to prevent avoidance. Social Security fraud seems to have retreated as an issue; it's the cutbacks to it which are capturing the public mind.

Chris Maltby - Softway Pty Ltd (chris@softway.oz)

PHONE: +61-2-698-2322 UUCP: uunet!softway.oz!chris
FAX: +61-2-699-9174 INTERNET: chris@softway.oz.au

Re: The Challenger and visionary software architects (RISKS-7.7)

The Polymath <hollombe@ttidca.TTI.COM>
13 Jun 88 21:13:42 GMT

}Date: Thu, 09 Jun 88 16:16:29 PDT
}From: Eugene Miya <eugene@amelia.nas.nasa.gov>
}Subject: Re: The Challenger and visionary software architects
}
}>From: stork@humu.nosc.mil (Kent Stork)
}>The May issue of Defense Science validates something that many computer
}>scientists have probably suspected: ultimately, the failure of the Challenger
}>and the death of the astronauts was due to a control loop software design
}>oversight - just another bug.
}
}The closest comment to "control loop software design" is:
} "It was not the leak that killed the astronauts. It was the
} attempt to correct the sidethrust, which sent the Challenger
} into violent oscillations.

This smacks of semantic quibbling. Had there been no leak there would have been no need to correct for it. In any case, the boost phase of the shuttle's flight is extremely critical with respect to forces on the assembled shuttle, tank and boosters. The shuttle's control surfaces are put through a very precise series of moves at this time to minimize stress all around. Any drastic deviation from expected conditions would be bound to have severe consequences.

} "If the Challenger had been permited to go off course,
} without attempting the major correction, the side booster would
} not have broken out, the booster would have burnt out with the
} Challenger still intact, and the crew could have ejected, off
} course but alive." [spelling corrected]

Not true. There were no facilities for crew ejection on board the Challenger. (A more feasible scenario would have been an attempt to fly the Shuttle to a landing after the boost phase had burned out). If the off-course shuttle had headed for a populated area the Range Safety Officer would have been in the unenviable position of having to destroy it _and its crew_ anyway. Fortunately for his peace of mind, he only had to destroy the boosters.

There are many RISKS associated with flying the Shuttle. While much effort is devoted to minimizing them, some of them simply have to be lived with.

The Polymath (aka: Jerry Hollombe, hollombe@TTI.COM)

Citicorp(+)TTI, 3100 Ocean Park Blvd. (213) 452-9191, x2483
Santa Monica, CA 90405 {csun|philabs|psivax|trwrb}!ttidca!hollombe

---

Academic Assignment of Viruses (RISKS-7.4)

John Gregor <unido!ecrcvax!johng@uunet.UU.NET>
13 Jun 88 21:09:43 GMT

-> Date: Sun, 5 Jun 88 10:25 EDT
-> From: WHMurray@DOCKMASTER.ARPA
-> Subject: Academic Assignment of Viruses

-> A society that depends upon any mechanism for its own proper
-> functioning, cannot tolerate, much less encourage, any tampering with
-> the intended operation of that mechanism.

Do you really believe that? Are you saying that any possible activity that could cause a deviation from the status quo is a danger and should be 'discouraged' (a euphamism for destroyed)? Unless you claim that the system is perfect (completely without flaw), how can you claim that an attempt to make change cannot be tolerated. Even if you feel perfection has been reached, who appointed you to be the conscience for the rest of the race? There no difference between your statement and worst actions attributed to "The Red Menace," in that they destroy the individual to maintain the purity of the state. Such closed mindedness never leads to an orderly society. It leads to the mindless destruction of all (both valid and fringe) criticism and methods of checks and balances. It leads to an ever tightening spiral of repressions that is only broken by revolution and chaos (not something I consider beneficial). Your statement is the antithesis of the ideals of personal liberty and social change that this (I'm a temporarily relocated US citizen, so I mean the US) country is founded upon.

-> Therefore, one is tempted to rise up in indignation at the idea of a
-> qualified academic assigning a virus to his students.

It's one thing to assign a project that specifically violates US or State laws. It is quite another to use an exercise to demonstrate the fallacies of system security, system design flaws, and the ingenuity and persistence of the dedicated. The assumed goal of the exercise was to give the students an insight into the problems of system security and design. A lesson they will take with them into industry to integrate into the next generation of computing systems. Then you and those like you will be praising the same people for their ability to seal up the leaks that plagued today's systems.

-> The next thing you know, they will be assigning plagiarism. How about
-> the forgery of academic credentials? Perhaps we should offer a course
-> in how to falsify research results. Or, perhaps, on how to trash
-> another's experiments, notes or reports.

This is in no way implied by the original project. It is only an

emotional appeal to create some sort of "mob-scene" reaction. It is in bad style. The sad part is that mob psycology works (mobs aren't very bright). This means that some external entity must apply force to the majority to protect the rights of the stampeding minority. From your posting and your ARPA location, I assume you are a part of some such entity. Unfortunately, the types that wind up ensuring the rights of the minority are also the most likely to mindlessly follow the state dogma and use their ability to use force to destroy the balances they were there to protect. It's a positive feedback situation. It's an auto-immune reation gone crazy. It's fatal. It's the biggest RISK of all.

-> Perhaps it is a sign of immaturity that we are unable to recognize the
-> moral equivalency. I will leave open the question of whether the
-> immaturity is in the technology, the society, or academia.

I sugest it is in those who fear any and all challenges to their dogma and supersticion. Especially those who fear ideas and use force to destroy them. Actually, I guess I'm no better. The basic philosophy your posting supports and what history has shown to be the results of that philosophy are the only cause I can imagine risking my life to help destroy. Our only difference is that I am able to live my life knowing that there are those who don't believe as I. While many of them won't rest until all of the heretics, perverts, and risks to their social order have been neutralized. Yes, this is a war. It's not one I would have. It's one that is caused by those who feel they MUST destroy all dissent and won't let the rest alone. I only hope I and the ones I love never have to fight.

-> I thought that we put this issue to bed several years ago when we
-> stopped assigning the breaking of security. It seems that we did not.

It's still common practice to stress test a system (computer, program, physics theory, etc.) by trying to break it. It's the only way to be sure. Why should a political theory or social order be sacrosanct? If you fail to test, unless you are perfect, the system will fail in a way that could have prevented if only the attitude of the powers-that-be didn't equate questioning as heresy. Our shuttle is a good example of where that attitude goes.

-> For an academic to be unable to recognize that assignments, and the
-> recognition that goes with their successful completion, encourages the
-> behavior assigned, demonstrates a lack of understanding of the activity
-> in which he is engaged. If he understands it, and still makes such an
-> assignment, he demonstrates a lack of understanding of where his real
-> interest rests.

-> Such irresponsible behavior may account, in part, for the anti-academic
-> bias in our society and for the manifest distrust of the scientific
-> establishment.

I believe that your perceptions of an anti-academic bias and distrust of academia stem from that fact that they can't be controlled. They can come up with facts independently from your personal belief system.

Your views are no better than the worst of the Soviet and Nazi system, where only state-backed results were released and non-conforming results were destroyed and the people involved "reeducated." Academia should have to bow to your (or anyone's) fears, superstitions, or idea of what the answers should be. Reality is not going to change, no matter how much you or anyone (creationists, flat earthers, etc) want.

-> It is of little wonder that the citizens of Cambridge, Massachusetts
-> are reluctant to trust the likes of these with genetic engineering.

An analogous project might be to create viruses and other biological agents that target "flaws" in the human system. I don't think you need to worry about the universities. The US military is quite advanced in this madness. The difference between the two projects is that

1. The computers are the property of the university and theirs to do with as they wish. Humans aren't.

2. An electrically and logically separate computer environment is easier to create/maintain and guarantees isolation. Biological systems aren't so simple or as easy to play with.

3. The worst case scenario for the computer project is: Brand X computers fall over until booted from a clean tape and some data is lost. For a biological scenario: Extinction of the human species or of all life on Earth. So why does the DoD continue Biowarfare? Or is is it ok because it's done by the state?

If I ever try to get a security clearance and this doesn't come back to me, I'll be disappointed.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 15

Tuesday 5 July 1988

Contents

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

"The target is destroyed."

Hugh Miller <HUGH%UTORONTO.BITNET@CORNELLC.CCS.CORNELL.EDU>
Mon, 04 Jul 88 11:15:52 EDT

There will be a board of inquiry, and congressional committees, and endless hearings, and in the end "operator mistakes" or "human error" will be found to have been the cause of the downing of the Iranian passenger airliner. A system as big and expensive as the Aegis cannot be allowed to fail, as the scandal about its testing revealed. The "failures" will be explained away.

The irony of this situation is, of course, that "human error" gets blamed for the disasters, to take the heat off the (more-infallible-than-the-pope) technology/-ists; but, in a skewed and entirely unfunny way the blame is well-placed. I imagine that every commander sitting in one of those high-tech bathtubs in the Gulf took one look at poor Captain Brindel of the Stark -- who took the fall and the forced retirement and the reduced pension when all along it was his buggy EW gear at fault, not he or his crew -- and said to himself, "OK, the writing's on the wall. If anything hits me and holes the ship & kills American sailors the pols will throw me to the sharks rather than admit that some whiz-bang from Rockwell or Unisys or whoever didn't do its zillion dollar job. So from now on it's hair-trigger 24 hours a day, and since I can't be sure my BOZO QZ999 Battlesys can knock down a missile once it's fired my only recourse is to knock the launchers down before they fire. They're bigger & slower & better targets anyway. Shoot first and ask questions later. The hell if I'm gonna be the next one to lose his Florida retirement condo to keep Marconi's rep clean." I can't find it in my heart to blame the man,

either. Who wants to be the fall guy for a gigabuck defense contractor and a desperate, freebooting White House in an election year? So along comes a jumbo jet, 25,000 feet, 430 mph, radar cross-section size of a football field. Software library in the EW battle computers says it's an F-14, kind that dinged the Stark. Hell, we ought to know our own aircrafts' profiles, right? You may fire when ready, Gridley.

So, in a way, it _was_ a "human" "error". A human, all-too-human error.

(Lest I be accused of imputing less-than-noble motives to valiant, dedicated career military men from my safe armchair half a world away, I advance for your consideration a hypothesis similar to the one Henry Spencer proposed, here or over in ARMS-D, I forget, last year. Never attribute to malice what can be accounted for by plain stupidity, he urged; I concur. Similarly, I would propose that one should not impute noble motives where base ones will do the trick, human nature being what it is. Remember, we live in a society where the most revered moral maxim is "Look out for Number One," followed closely by "Cover your ass" and "Nice guys finish last." Naivete, especially willful naivete, is not a necessary condition of lucidity in thinking about techno-political matters. And, today, all technological matters are political and vice versa.)

Which brings me, Mr. Speaker, to my questions. They are not original, but since they have never been answered and still seem crucial I will put them again.

1: Surely one of the greatest risks at which we are held by technology is the result of its completely self-contained, hermetic world-view? In that view, all nature, human and otherwise, is a machine, science the search for the control levers, and technology the pulling thereof. We are guided in how we want to pull them by our "values," whatever they are. (What are they, by the way, in the Persian Gulf? I suppose the usual "national interest," whatever that is.) Just as we don't stop using our PC because the disk drive breaks -- Quick! Get the drive repaired! --technological thinking will not countenance any stint of its advance. Greenhouse effect? Engineer hardier crops. (I heard _that_ one at the Toronto atmospheric conference the other day.) 290 dead civilian airline passengers, including 66 children? Patch the software library, piece of cake. Six months from now, when we shoot down a couple of our own fighters returning from a sortie because of an unforeseen bug in the Flight 655 patch, we patch the patch, no problem. Nothing fazes the true believer, except the suggestion that we deep-six his favorite toy.

2: Technology creates risks, vigorously. Since politics and technology are today joined in unholy matrimony, technology creates political risks. Techno-freaks don't like to think about this, preferring to pretend to be "apolitical" so no one will disturb their tidy world, but it is no less true or all that. Since World War II especially the military has been the hot spot for the interpenetration of politics and technology. Only the can-do technoptimism of the postwar armed forces can explain such patently politically imprudent and hazardous ventures as the Persian Gulf filibuster or the "600 Ship Navy"'s aggressive forward basing strategy, to say nothing of CBW or, haha, the Strategic Defense Initiative. The bigger and more optimistic the technology, the bigger the risks. Soviet SSBN's

off Virginia and Pershing II's in Europe? An 8-minute LUA decision window. This is not, _pace_ Charles Perrow, a matter of "normal accidents" arising out of the increasing complexity of systems. It is a _positive drive_ coeval with technology itself, to which the complexification problem is only an adjunct. As Oppenheimer once told us, "If the experiment is sweet, you have to run it." If there's no going back, are we prepared for the increasingly wild lurches politics will take in the nearer and nearer future?

Hugh Miller, University of Toronto,(416)536-4441

Clarifications on the A320 Design

Nancy Leveson <nancy@commerce.ICS.UCI.EDU>
Sun, 03 Jul 88 19:00:12 -0700

There has been a great deal of speculation about the design of the A320 computing system in Risks. I would like to clear up a few things. First, the A320 is not designed like the F-16 or Boeing 757/767. The information below is taken from a paper by J.C. Rouquet and P.J. Traverse entitled "Safe and Reliable Computing on Board the Airbus and ATR Aircraft," which was published in the Proceedings of Safecomp '86 (Safety of Computer Control Systems 1986), edited by W.J. Quirk, published by Pergamon Press, and copyrighted in 1986 by IFAC (International Federation of Automatic Control). The authors work for Aerospatiale, the firm responsible for designing most of the computing systems on board Airbus aircraft. I quote from some of the relevant parts; sorry I could not include the figures. Instead of trying to correct the English in the paper (which was obviously not edited before printing), I have left it as is for accuracy; I have tried to proof read this typewritten message carefully to make sure that I have not introduced errors. I apologize if I have.

... "The A320 is the first civil aircraft designed as fly-by-wire. It is also the only aircraft with such an ultra high reliability requirement (failure rate of 10^-9/H) for a computing system." ...

"Safety-only requirements can be specified as not computerized back-up exits. Let us take the roll control of the AIRBUS 300-600 and 310 as an example. The aircraft is controlled on the roll axis using a pair of ailerons and 5 pairs of spoilers. The aircraft is controlled either in manual mode, or in an automatic one. The automatic flight control system is composed of two "Flight Control Computer". Only one of them is active at a time, the other one being a spare. If both computers are lost, the aircraft is manually controlled. Therefore, the loss of the automatic flight control system is not dangerous for the aircraft (except during a short period of an automatic landing in bad weather conditions)."

"Computers are involved in the manual control mode. Two "Electrical Flight Control Unit" are used to control the spoilers. If both computers are lost, the pilot can still control the aircraft using the ailerons, with a reduced authority, as the spoilers are no more available."

"The basic building block is a duplex computer. Each high safety computer is composed of two computation channels. Each channel is monitoring the other. If one channel fails, the other one shuts the whole computer down in a safe way. This scheme can be impaired by a latent error of the monitoring. Therefore, a self-test program is run each time the computer is powered up."

"Other precautions are that each channel contains watchdog, that exception testing and acceptance testing on the channels output are done, and that if a computing channel contains two processors, they partially cross-check themselves."

"Input to the computer are also tested prior to use. It has to be noted that safety is not affected, even if a Byzantine general strikes. Indeed, if a sensor sends different information to the two computation channels the consequence is only the shut-down of the computer."

"As a basic precaution, computers are shielded and loosely synchronised. Most of the transient are coming through power supply. Therefore, the power supply is filtered, but also monitored. A power loss is thus detected, a few data stored in a protected memory. If the power loss is sufficiently short, a "hot start" is possible. Else, the computer can anyway reset itself, and restart."

"Equipment on board are divided into two subsets. These two subsets are often referred the 2 sides of the aircraft. Typically, one side is controlled by the pilot, the other by the copilot."

"The main characteristics are as follow:
 -- only one side is needed to flight [sic] without almost any limitation
 -- an error cannot propagate from one side to the other
 -- a fault cannot be common to both sides
The main task is to verify that the two sides are sufficiently segregated to limit error propagation and common point failure."

"High quality software is obtained using a quality plan, as defined in (DO178A). [I discuss this standard, and my qualms about it and the n-version programming used to justify the high reliability numbers, in a previous Risks. It was reprinted in SEN. NGL] This document is agreed as a basis for certification. Its recommendations are used during the software design phase, and each time software must be recertified because of modifications."

"This (and any) rigorous design and testing methodology is not acknowledged as a fault free software warrant."

"Therefore, each computers uses two different programs, one in each channel. The dissymetry (diversity) between the two programs is obtained using:
 -- different software design teams,
 -- different languages,
and, depending on the computer, different algorithms, functions, etc.."...

"A major concern is about maintenance faults. Their effects are limited, thanks to the power-up self tests, and the computer aided maintenance system.

The pilots are generating input to the computers, and it is recognized that in most of the accidents, at one time, a pilot takes a wrong option. This error may not be an important one, and it has to be noted that in these cases, the pilot is generally in very bad working conditions. Anyway, pilot errors are a major concern. Two ways to cope with these are:
-- a computer aided decision (in case of emergency) system (Airbus 300-600, 310, 320)
-- a limitation of the authority of the pilot (A320)."

"The first system called Electronic Centralized Aircraft Monitoring displays adequate procedures on a screen.... More, on the A320, the pilot cannot drive the aircraft outside the flight envelope. [Wasn't this what the manufacturers claimed happened in the recent accident? NGL] Ziegler and Durandeau (1984) have discussed further this point. " [Citation to a paper entitled "Flight control system on model civil Aircraft, Proc. of the International council of the Aeronautical Sciences (ICAS '84), Toulouse, France, Sept. 1984.]

"The flight control of the A320 is ensured by a computing system, with a limited mechanical backup. The design objective is for the computing system to be sufficiently reliable in order not to use the mechanical back-up. This back-up is on board to ease the certification of the aircraft and to help people to be confident in the aircraft."

"The safety requirement still exists for the computers. Therefore, they are built following the rules defined above (two channels computer, different programs, high segregation ...)."

"Reliability is gained using five computers. All of them participate in the control of the aircraft on the roll axis, four of them on the pitch axis. At each time, each surface is controlled by one computer, the other being hot back-up. Two types of computers are used. One is called 'ELAC' (Elevator and Aileron Computer) is manufactured by THOMSON-CSF, around microprocessors of the 68000 type. The other is built by SFENA and AEROSPATIALE with 80186 type processors, and is called 'SEC' (Spoiler and Elevator Computer)."

"Each computer has two different programs. Therefore, two types of computer have been designed and four programs. The repartition of the computers is shown on Table 1."

	PITCH	ROLL	'SIDE'
ELAC 1	x	x	1
ELAC 2	x	x	2
SEC 1	x	x	1
SEC 2	x	x	2
SEC 3	-	x	2

TABLE 1 - Repartition of the computers

"With this architecture, the aircraft can tolerate:
-- multiple hardware failures
-- a complete loss of one 'side' of the aircraft
-- at least a software error, or a hardware design error, event if it shuts down one type of computer
-- combinations of the above."

"More details about the Electronic Flight Control System of the A320 can be found in a paper by Ziegler and Durandeau (1984)." [Cited above]

"When an equipment fails, two problems appear. First, to find it, and second to replace it. On the A320, the localization is done at two levels: each equipment records failure indication, and at the aircraft level, a computer collects all the information and correlates them. It is thus possible to have at a terminal the list of all the failed computers, through the 'Centralized Fault Display System.'"

"Spare parts are not available in all the airports. In order not to ground an aircraft, it is needed to have spares on board, or for the aircraft to be able to take off with failed equipment. The second way is taken and computing systems are generally designed to reach their the [sic] reliability requirements, even if one of the computer is down. For example electrical flight control system of the A320 is composed of five computers, but, provided some limitations of the flight envelope, it will be allowed, and safe, to take-off with only four computers up."

... "The demonstration [of the assigned reliability] is based on ground or flight test (to measure the effect of a failure), on probability numbers, and on a software design quality plan in accordance with (DO 178A). No number is assigned to a software, even if measures have been done by Troy and Baluteau (1985)." [Reference to a paper in the proceedings of FTCS-15, June 1985, pp. 438-443].

"The 'Zonal Safety Assessment Document' analyzses the effect of such things as an engine burst, waste liquids, ..."

"We rely also on ground and flight tests. For example, the equipment of the A320 are tested on ground in an 'iron bird' for one year prior to the first flight. During the year between the first flight and the certification, both ground and flight tests will be performed. The ground tests include power supply transients, electrical environment hazard."

[There is a section on accrued experience] ... "Our record is satisfactory. No aircraft crashed, and even came close to this situation. Design errors have been found in operation, both in computer specification, and in programs. We plan to examine all of them, but at first glance, none of them is dangerous. The use of design diversity is successful, as no error has been found in both versions of a software."

NGL: The argument in Britain about the A320, led by Mike Hennell and Bev Littlewood, has focused on the lack of proof of the claims by the manufacturers of the Airbus A320 that they have the safest plane flying because of the ultra-high reliability of the computer systems. Despite the claim of 10^-9/H, there was an incident where the A320 computers all failed in test. The manufacturers explain this as a "teething problem" that will disappear after test. They also stress that the test pilot was able to safely land the plane on the back-up system.

I have been concerned about claims that the use of n-version programming (aka "design diversity") will provide ultra-high reliability. John Knight

and I have written several papers describing experiments with this technique. Tim Shimeall and I have also just completed another experiment that compares n-version programming and more traditional reliability techniques. I will send anyone copies of these papers upon request.

Let me add to the voices suggesting that we wait for the final data before judging the latest accident. In almost all accidents, the manufacturers of the equipment involved immediately claim that it was a result of operator error (for very good reasons which are usually of a liability and monetary nature). It did not seem like the pieces had all stopped smoking before the cause of the A320 accident was announced. Unfortunately, with the immense amount of money involved, it is not clear that the truth will ever be known. If it truly is a technical problem, it may require multiple accidents and deaths before this is admitted. This, by the way, is what happened with the Therac 25. It now appears that some early accidents involving the Therac 25 were the result of software error even though hardware was blamed in the official accident reports. After several such accidents, it was no longer possible to continue to blame the operators and the mechanical systems, and the software errors responsible were finally found. The Three Mile Island accident is often attributed to operator error although four separate hardware failures occurred before the operators even got into the act. Most accidents are not attributable to a single cause -- they are a result of the interaction of several factors. It is always possible to blame the operator for not taking the correct steps to "save the day" after the accident scenario has already been started; accidents in complex systems are usually not a matter of operator error alone. At the least, why was the system involved designed to be unsafe on a single point failure like an operator error? If it is, then the limiting reliability is that of operator error, which is usually counted as 10^-5 in risk assessments. Note that according to the paper cited above, the A320 contains a computer-aided decision system and a limitation of the authority of the pilot. The pilot also cannot drive the aircraft outside the flight envelope. If this is true, it seems odd to blame the recent accident solely on the pilot driving the aircraft outside the flight envelope, as reported by the press.

Virus aimed at EDS gets NASA instead

Dave Curry <davy@intrepid.ecn.purdue.edu>
Mon, 04 Jul 88 11:18:37 EST

Taken from The Lafayette Journal & Courier, 7/4/88, Page A2.

Destructive computer program sabotages government data

NEW YORK (AP) - A computer program designed to sabotage a Texas computer company destroyed information stored on personal computers at NASA and other government agencies, according to _The_New_York_Times_.

It was not known whether the program had been deliberately introduced at the agencies or brought in accidentally, but NASA officials have asked the FBI to enter the case.

Damage to government data was limited, but files were destroyed, projects delayed and hundreds of hours spent tracking the electronic culprit.

The rogue program destroyed files over a five-month period beginning in

January at the National Aeronautics and Space Administration, the Environmental Protection Agency, the National Oceanic and Atmospheric Administration and the U.S. Sentencing Commission, the _Times_ reported.
The program, or virus, infected close to 100 computers at NASA facilities in Washington, Maryland and Florida.
The virus was designed to sabotage computer programs at Electronic Data Systems, a private company in Dallas, Bill Wright, a company spokesman, said. The program did little damage, he said.

--Dave Curry
Purdue University

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 16

Wednesday 6 July 1988

Contents

- Air France Airbus A320 Crash Story In Aviation Week
  Karl Lehenbauer
- Common failure path in A320
  Lee Naish
- Reply to Hugh Miller about Iran Flight 655
  Michael Mauldin
- The Iranian airliner tragedy
  Bob Estell
- Aegis and the Iran Airbus
  PGN
- The "F-14" attacking the Vincennes... But the F-14 is for air defense
  Jonathan Crone
- It's easy to make decisions if you don't have the facts
  Martin Minow
- Re: A300 using F14 transponder
  Bruce O'Neel
- Iran Flight 655 and the Vincennes
  James P. Anderson
- Lockpicking
  Randy D. Miller
- Re: The Eyes Have It
  Tracey Baker
- RISK of PIN's - PNB calling card
  Scott Peterson
- Info on RISKS (comp.risks)

Air France Airbus A320 Crash Story In Aviation Week

Karl Lehenbauer <sugar!karl@uunet.UU.NET>
6 Jul 88 01:19:18 GMT

(quoted without permission from the July 4, 1988 issue of Aviation Week)

"The investigation into the June 26 crash of an Air France Airbus Industrie

A320 is focusing on the pilots' judgment in performing a slow-speed air show flyby with a fully loaded transport that they allowed to descend well below their filed minimum altitude."

[background information on the crash deleted for brevity]

"Video images of the accident showed that the A320 was stabilized in a nose-high attitude throughout the flyby, and that the mid/aft section of the aircraft struck the outermost row of trees at the perimeter of the airport. The aircraft then settled into the wooded area and burned.

The pilots said they thought the aircraft was at an altitude of 100 ft. based on the flight instruments, and stated that the A320's two CFM International CFM56 turbofan engines did not respond correctly when they moved the throttles forward for full power."

[The article goes on to quote the French Transport Minister Louis Mermaz and later the Director of the Direction Generale de l'Aviation Civile (DGAC) as saying that the aircraft's 30-ft. flyby altitude and its reduced airspeed "were confirmed by both the cockpit voice recorder and the cockpit data recorder."]

"'When the pilot advanced the throttles, the thrust was increase was normal, but it [the power increase] apparently was made too late,' Tenenbaum said. 'This is important because the pilot reported after the accident that the engines did not respond. ... According to the data, the thrust increase to the full available power should have occured within 8 sec., and we saw it in approximately 5 sec.,', he said."

[The article then describes the renewal of a long debate in France over the minimum crew requirements for the A320.]

"'Based on the cockpit conversations we heard [on the cockpit voice recorder], the crew was perfectly aware of what was going on,' Tenenbaum said. 'They were perfectly lucid, they knew what altitued they were at because there were [computer-generated] voice callouts from the radar altimiter during the low pass, including an audible callout of 30 ft.'"

[The article proceeds to describe the orientation of the aircraft during its low pass and as it struck the trees (nose-high level flight), the history of Air France's operations of the aircraft, that Air France has decided to suspend all further demonstration flights and that British Airways and Air France substituted other aircraft for their scheduled A320 flights for two days after the accident.]

"Officials at British Airways said the airline had experienced no significant mechanical or electronic problems with the aircraft since they entered service earlier this year.

Several European test and company pilots questioned the crew's reasoning in attempting to perform an air show-type low, slow flyby without apparent advanced training and with a passenger payload."

Common failure path in 320

Lee Naish <munnari!mulga.oz.au!lee@uunet.UU.NET>
Wed, 6 Jul 88 19:00:14 EST

Though the A320 Airbus has redundant computer systems, they all use the same air conditioning system. Does anyone know what the expected failure rate of that system is, or how critical a failure would be?

Lee Naish

Reply to Hugh Miller about Iran Flight 655

<Michael.Mauldin@NL.CS.CMU.EDU>
Tue, 5 Jul 1988 22:38-EDT

I can't match Mr Miller's polemic, but I can point out that he got just about every fact wrong about flight 655. All of the information below is from the Pittsburgh Post Gazette, Monday July 4. Their text comes from an article by Stephen Engelberg of the New York Times News Service.

> So from now on it's hair-trigger 24 hours a day, and since I can't
> be sure my BOZO QZ999 Battlesys can knock down a missile once it's fired
> my only recourse is to knock the launchers down before they fire. They're
> bigger & slower & better targets anyway.

Do you have a problem with that? You criticize "the system" for overreliance on technology and then fault the captain for his caution?

> Shoot first and ask questions later.

3 warnings were radioed on civilian distress frequencies
4 warnings were radioed on military frequencies
A nearby Italian vessel reported hearing at least 4 of these warnings

All of the discussion I've heard said that he should have fired 2 minutes earlier, and would have been justified in doing so, given the information available. Captain Rogers was very forgiving to have waited as long as he did.

> The hell if I'm gonna be the next one to lose his Florida retirement condo to
> keep Marconi's rep clean." I can't find it in my heart to blame the man,
> either. Who wants to be the fall guy for a gigabuck defense contractor and a
> desperate, freebooting White House in an election year?

How about a more likely line of reasoning:

"Gee whiz, just after we sank two of those gunboats this plane takes off from a nearby civilian/military air base and is closing directly on my ship. It has no transponder and won't answer my radio challenge. Maybe I should shoot it down to save

my ship and the men in my command."

> So along comes a jumbo jet, 25,000 feet, 430 mph

An A300 is much smaller than a jumbo jet.
It was flying at 9,000 feet and descending. It was shot down
at an altitude of 7,500 according to Iranian press releases.
It was traveling 450 knots (518 mph) and gaining speed.

> radar cross-section size of a football field.

The wingspan of an A300 is 147 feet, less than half the size of a football field. That's a little more than twice the 64 foot wingspan of an F-14. In any event the bottom line is that you can't reliably identify planes from a head-on cross section. No one has ever said they could.

> Software library in the EW battle computers says it's an F-14, kind that
> dinged the Stark.

The plane was tentatively identified as an F-14 not from radar but from five other facts:

1. There were reports of 10 F-14's operating out of Bandar Abbas.
2. The flight took off from Bandar Abbas immediately after the Vincennes fired on the three gunboats.
3. It had no transponder (a requirement for all civil aviation).
4. It was 4 miles outside of the commercial air corridor and 14,000 feet lower than a commercial plane should have been.
5. The plane was broadcasting on a military "mode 2" (I'm not sure whether that's a radar or a radio). These were the "electronic indications" the Admiral Crowe spoke of in his press conference. (This comes from CNN news Tuesday, July 5).

Also, Flight 655 took off about an hour after it's scheduled departure time; the captain had requested information about scheduled commercial flights, but this search was not completed before the decision to fire was made. Even if they'd had the time, all they would have found was that it was the wrong time to be a commercial flight. (Also from CNN News).

It may well be true that the Iranian pilot thought our technology was so good that we could identify him properly despite the fact that he was in the wrong place at the wrong altitude at the wrong time ignoring (or unable to hear) frequencies he was required to monitor. To that extent there may well have been an over-reliance on our technology.

---

the Iranian airliner tragedy

"FIDLER::ESTELL" <estell%fidler.decnet@nwc.arpa>
6 Jul 88 08:21:00 PDT

The "target is destroyed" note in RISKS 7.15 of 5 Jul 88 was not pleasing to MY tastes; whether it was in good taste or not is a question that I won't raise; tastes are far too personal for rational debate. I know our moderator personally, and I trust his judgment.

But I also know CAPT Will Chapel Rogers III; we had two years together at Baylor a long time ago. The traits that made Will a friend and a good student are ones that the Navy seeks in recruits, and develops in officers; I cannot believe that the goodness has been trained out him.

I also know a thing or two about Aegis radar systems, F-14's, C3 systems used in Navy combatants. I know for instance that the "radar signature" of a "loaded fighter-bomber" [or other medium aircraft, carrying missiles] can look as large as a jet liner, for much the same reasons that a sequined bikini will reflect as much footlight as a white satin gown. And I learned Tues 5 Jul p.m. that the Iranian airliner was identifying itself as an F-14. The Vincennes fired for much the same reasons that the police in many cities fire at apparently armed assailants almost every day: self defense. When it sometimes happens that afterwards the attacker turns out to be relatively innocent [e.g., kid with a water gun], that's a "tragedy."

One of the RISKS of using computers is that we sit in our cubicles and deal with machines - that feel no pain, leave no widows nor orphans; we come to think of human loss as statistics, which we compute so easily. The loss of one life is tragic; 290 at a stroke only serves to awaken our dulled senses!

Tragedy is one thing; justification is another. I happen to believe in self-defense, an adequate army [and navy], and capital punishment. But I repeat, the loss of human life is tragic. Let's not rush to judgment just because the statistics get our attention. Instead, let us resolve [in Lincoln's words] that these 290 will not have died in vain: Let us rethink both our [computerized] weapons systems designs, AND their use.

Bob
p.s. The opinions herein, as always, are personal; NO conclusions can be drawn about my employer's concurrence or lack thereof.

It's easy to make decisions if you don't have the facts

Martin Minow THUNDR::MINOW ML3-5/U26 223-9922 <minow%thundr.DEC@decwrl.dec.com>
6 Jul 88 13:34

Idle speculation: sometimes it's more interesting to listen to what wasn't said. In the recent attack on the Iranian airliner, why do I get the feeling that nobody on the Vincennes was monitoring tower-plane radio communications. (And the vague suspicion that there wasn't anyone on the ship fluent in Farsi.)

Martin Minow

Re: A300 using F14 transponder

Bruce O'Neel <XRBEO%VPFVM.BITNET@CUNYVM.CUNY.EDU>
Wed, 06 Jul 88 08:09:10 EDT

[Referring to the Mode 2 / Mode 3
confusion, and belief in the transponder:]

Seems it might be a good idea in a war to equip all the fighters with transponders saying that they are say 767s?

Aegis and the Iran Airbus

Peter G. Neumann <Neumann@KL.SRI.COM>
Wed, 6 Jul 88 10:40:16 PDT

An article in this morning's San Francisco Chronicle (p. A-12) is titled

"Electronic Errors

Star Wars Planners' Lesson in the Gulf", by David Perlman

[...] The cruiser's Aegis system linking its radar with a battery of advanced comptuers and missile launchers, had been hailed as "Star Wars at Sea" by the Navy. But David L. Parnas [...] held a different view. "It is obvious," he said in an interview, "that if you can't discriminate at close range between an Airbus and an F-14 fighter, it would surely be even more difficult if not impossible to discriminate between a Soviet warhead and a decoy baloon flying on the same ballistic trajectory in outer space." ... "The Aegis system was always presented to me in briefings as a defensive system only against high-speed, low-flying missiles," Parnas said. "But, while I have no reason to believe that it was the Aegis computer system that failed on Sunday, the fact is that discriminating targets is vital for any defense."

The "F-14" attacking the Vincennes... But the F-14 is for air defense

Jonathan Crone <CRONEJP%UREGINA1.BITNET@CORNELLC.CCS.CORNELL.EDU>
Wed, 06 Jul 88 10:30:47 CST

I basically have a comment to make about the supposed response about the Vincennes defending itself against an attack from an inbound F-14.

Were the F-14's that were sold to Iran during the 1970's stock F-14's or were they supplied with upgraded avionics and attack systems.

The reason I'm questioning this, is because Grumman designed the F-14 to support the Navy's requirement for a powerful Air Defense Fighter.

This explains the F-14's exceptional ""capabilities"" in this area... (such as the supposed ability to maintain lock on 24 inbound targets and to attack 6 of those targets using a mix of Phoenix Sparrow/AMRAAM, and Sidewinder missiles.)

However, and I recall this from reading material published during the late

seventies when Canada was looking to purchase a new all purpose fighter for the Canadian Airforce, the F-14 has very limited Air to Ground capabilities... its radar and attack systems aren't really designed to do it. (thats why Canada purchased F-18s instead, because it had multipurpose radars to deal with both modes of combat.) (The Canadian Air Force required a single type of aircraft that would be capable of dealing both with the close ground support environment of NATO commitments, as well as the long ranging Air Defence requirements over North America)

Presumably the crew of the Vincennes would know about this wouldn't they??? (from news reports, Iran, is still using F-14's as Air to Air units, and not as ground attack birds.)

If I were the Commander of the Vincennes, I would be worried if the Aegis was saying that the inbound aircraft was a Mirage or a Super Etenard (a Mirage is the aircraft that launched the two Exocet missiles that holed the Stark).

So perhaps the big question is, why are they saying that they were worried about the possibility of an attack from an F-14?

Jonathan P. Crone

Iran Flight 655 and the Vincennes

<JPAnderson@DOCKMASTER.ARPA>
Tue, 5 Jul 88 23:03 EDT

The Captain of the Vincennes did the correct thing. If he can be faulted for anything, it is that he waited so long before acting. All the breast-beating in world and appeals to castigate the military notwithstanding, the correct action was taken. If a human failure took place, it was in the Iranian decision to fly a commercial aircraft over an area where a fire-fight was in progress, and in not responding to the reported 7 (repeat seven) attempts to raise the aircraft and have it identify itself. The loss of life was indeed tragic. The attempt to picture the U.S. Navy or U.S. policy as irresponsible is even more tragic.

Mr. Miller seems genuinely confused over what is 'national interest'. I would submit 'national interest' is Canada selling its wheat to anyone it chooses regardless of what other nations; ostensible allies and maybe even friends, think. It is also an assertion that a tin-horn dictator, operating under the guise of religious leader cannot prevent free ship movement in the Gulf area. It is possibly also a belief that the rest of the world, maybe even Canada might suffer if oil does not move freely from the Middle East. [I guess the view of 'national interest' is crystal clear from the lofty towers of academe.]

Let's get the forum back to technical risks and off of the political beat. Jim

---

Lockpicking

Randy D. Miller <sun!sunburn!gtx!randy@ucbvax.Berkeley.EDU>
Tue, 5 Jul 88 09:44:06 MST

I never imagined that picking locks could be so easy. A couple months ago, I went to the Phoenix Public Library (!) and checked out a few books on locksmithing. Surprise! The books all had chapters on how to pick locks for fun and profit. One book explained how to make homemade lockpicks by grinding down hacksaw blades. Using $0.99 hacksaw blades and a Dremel Tool grinder, I made an assortment of lockpicks. K-Mart supplied me with an assortment of locks to practice on and disassemble.

After a few days of practice, I found that I could pick open any disk tumbler lock that I could find - these are the cheap locks found on desk drawers, cabinet locks, window locks, and a few cheap padlocks and old door locks. Most disk tumber locks take me less than 10 seconds to get open. I've also picked open every pin tumber lock that I've tried, but they're harder; most of them take about two minutes to get open. These are the locks found on most doorlocks. The most difficult lock I've tried is the expensive Master brand pin-tumbler padlock, which required about twenty minutes of delicate work to pick open. (I disassembled it to see why it was so hard. Master uses smaller pins than usual, made to very tight tolerances, without the bevelled ends found on most pins.) There are such things as pick resistant locks, but they are pretty rare. It seems that 99 per cent of the locks in my life are pickable disk tumbler or pin tumbler locks. (I haven't yet begun practicing on automobile locks; from the diagrams in the books, they seem to have extra features that may make them harder to pick.)

I called some city and state offices, and one local locksmith, to see if there are any laws regulating the possession and use of lockpicks in Arizona. No one I talked to seemed to know anything about any regulations!

If it's so easy to pick open locks, why do burglars resort to harder and messier ways of entering buildings, desks, cabinets, etc.? Are most burglars incapable of learning such a skill, or does it just not occur to them? Should I spend a fortune replacing the locks on my house, or are the risks low that a burglar will pick the locks?

Randy D. Miller (602) 870-1696
GTX Corp., 8836 N. 23rd Ave., Phoenix, AZ 85021
{cbosgd,decvax,hplabs,amdahl,nsc}!sun!sunburn!gtx!randy

[One of the imperative themes in the RISKS Forum is that protection measures are inherently compromisable. The myth of technology as a panacea continues to haunt us. Most car-door locks are TRIVIAL to break. Skeleton keys for house locks are simple to fabricate. Cyclic redundancy checks and crypto seals are simple to break if the underlying system is not adequately secure. Thus using a complicated mechanism on top of a flawed mechanism invites compromise. The more sophisticated the lock mechanism, the more challenges for the sophisticated attacker. But the belief in technology as a magic wand is perhaps the most dangerous of all -- whether it is locks or automated defense systems. PGN]

Re: The Eyes Have It (RISKS DIGEST 7.14)

<tab@mhuxu.att.com>
Tue, 5 Jul 88 17:32 EDT

I had to laugh at "The Eyes Have It". The last five digits of my NJ driver's license number are 61664. This is supposed to represent my date of birth and eye color. I was born on 11-22-66, and the last time I checked my calendar, we didn't even have 61 months!

This made me think about PGN's comment about three extra "eye color" values not being enough to prevent data collisions. Since it is obviously possible to have the first "DOB" digit not match the actual DOB, why not use 2-9 in that field? That, combined with the extra eye color values, would leave room for almost eight times as many "identical" people ("almost" because Jan-Nov and Feb-Dec birth dates would have to share the extra numbers). They could still retain the DOB information if 2-5 in the first digit = 0 and 6-9 = 1.

It also makes me wonder about the NJ DMV. I know they've had many problems with their computer system (and their offices, and their personnel, and ... :-), but this is ridiculous - not only do the two DOB fields not match (they did get it right in the DOB space on the license), but one of them isn't even a valid date!

(If the NJ DMV already uses different DOB #'s for data collisions, I apologize for this entire article. I've *never* heard of anyone else with something other than the DOB in those 4 digits. In fact, everything I have heard makes my nuber look like a unique case. If there were a reliable way to get information from the DMV I'd ask them, but they can't even tell me what forms I need to register my car, so I'm afraid there's not much hope of getting a correct answer to a question like this.)

Tracey Baker {att, rutgers!moss}!mhuxu!tab or tab@mhuxu.att.com (201)582-5357
Rm. 2F-211, AT&T Bell Laboratories, 600 Mountain Ave., Murray Hill NJ 07974

RISK of PIN's - PNB calling card

<littlei!foobar!sdp!sdp@uunet.UU.NET>
Tue Jul 5 20:46:53 1988

After noting charges on my last phone bill for calls made from places I've never been, I called Pacific Northwest Bell (PNB) and changed the PIN on my calling card. (I decided to pay the $3 in long distance charges since I had given my PIN to an old girlfriend about a year ago.)

I was mildly surprised to find that the procedure for changing my PIN was to tell the PNB representative on the phone what I wanted my new PIN to be. I already (have to) trust the phone company, so this risk was acceptable to me.

I was REALLY surprised by what I found out when I received a new calling

card in the mail today. (Probably sent automatically because I changed my PIN.) Here are some of the "features" of my new calling card as explained in the letter sent along with it:

> "Exclusive extra security
>
> When you look at your Card, you'll notice that your four-digit security number is not shown. That means _extra security for you_, because only you know the Security Code.
>
> Maximum convenience
>
> Turn your card over. The magnetic stripe on the back lets you use many of the new Card Reader phones. _You don't need to enter your card number or your security code_. Just slide your Card through the special slot and dial! ... "

Identifying the problem with this is left as an exercise for the reader.

I think I'll just hit my card with a bulk tape eraser, and forget about using card reader phones until PNB straightens this out.

Scott Peterson, OMSO Software Engineering, Intel, Hillsboro OR
sdp@sdp.hf.intel.com uunet!littlei!foobar!sdp!sdp

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 17

Friday 8 July 1988

Contents

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

Politics and Risk

Gary Chapman <chapman@csli.stanford.edu>
Thu, 7 Jul 88 16:27:06 PDT

I would like to respond to the contributors who suggested that we "leave politics out of" this forum, and stick to "technical" subjects. These comments were in response to a contribution from someone from the University of Toronto, who was highly critical of the use of computer-based electronic systems like the one that was involved in the Iranian airliner tragedy. I for one found his first RISKS posting on that subject very cogent and appropriate.

If this forum is to address the risks of technical systems, it seems highly artificial and misleading to eliminate consideration of the political

environment the potentially risky system may be in. RISKS readers should certainly be spared pure political harangues or ideological tirades, but there is no reason why we cannot consider a technical system's political environment part of the mix of ingredients that may make it risky. Indeed, for some systems it is almost exclusively the combination of the technical character of the system and the political environment within which it is meant to work that constitutes the risk. The Strategic Defense Initiative would pose considerably less risk, perhaps even close to zero, if it did not have to cope with hostile nuclear warheads (and of course the entire raison d'etre of this system is bound up with politics). The technical reliability of Navy shipboard radars and other sensors is of paramount importance precisely because they are operating in a combat zone. If the system's reliability, or unreliability, has large and grave implications for the political environment in which it is working, it should be within the purview of engineers and technologists to question the wisdom and prudence of introducing the system into such a political context. This is simply analogous to a matchmaker suggesting that his product not be used around gasoline or dynamite without due caution.

Extrapolating from that, it is certainly part of a comprehensive assessment of risk to ask questions about why we want whole classes of technical systems, such as increasingly automated weapons, weapons that destroy things faster or more thoroughly, etc., when these technical capabilities entail not only risk in the conventional sense of malfunction, but "social risk" in helping to usher in a nightmarish world that our children will probably regret. It is legitimate consideration of this "social risk" that many engineers and technologists avoid like the plague--it is labelled "emotional," "irrational," "not technical," etc. It is astonishing that this is so widespread among technical professionals when the "social risk" of so many technologies is so readily apparent in our age, and appears to be getting generally worse instead of better.

During the war in Vietnam, the United States Air Force had virtually unchallenged air superiority, and we dropped three times more bomb tonnage on Southeast Asia than was used by all the powers in all the theaters of World War II. This almost unimaginable destruction didn't do much of anything in terms of winning the war or even furthering short-term American military objectives. The North Vietnamese still won the war, despite devastation the contemplation of which would make many people permanently catatonic (for a description of this madness, read James William Gibson, *The Perfect War: TechnoWar in Vietnam*, Atlantic Monthly Press, 1986, Part III, "Death From Above"). The Pentagon Papers revealed that the Air Force knew the saturation bombing was having no effect on the level of resistance of the enemy. The Air Force knew this, and yet recommended *escalation* of the bombing throughout the remainder of the war.

Was this a technical problem of not hitting the right targets, or not working out the right pattern of bombing sorties? Was this the "correct" decision by Air Force commanders who were given a job to do with a certain tool? As the saying goes, "if the only tool you have is a hammer, all problems begin to look like nails." If we give Air Force commanders lots of big B-52s and lots and lots of 500 and 1,000 pound bombs, should we blame them for attempting to turn most of Southeast Asia into a parking lot?

Or was this a "social risk" of the technology, an atrocity in which all people

are implicated, technologists and "end users" alike? Can the technology itself have a role in creating the political context in which the technology itself rockets risk over any scale we had previously imagined? This is what happened with nuclear weapons, and now it's happening with a whole spectrum of technologies that are becoming increasingly refined and increasingly deadly.

It's pointless and even distasteful to address these issues in purely technical terms. To address risk in that fashion is to limit oneself to "tweaking" systems that may be fundamentally wrongheaded to begin with, technological systems that, at their core, are bad--not just risky--for humanity. Some may think that this adds up to an "emotional" appeal, but there's nothing inherently wrong with that. It takes people with emotion, and not just a facility for algorithms, to recognize risk and to do something effective about it.

Gary Chapman, Executive Director
Computer Professionals for Social Responsibility chapman@csli.stanford.edu

---

Iranian Airbus ([mis]quotation from the SFO Chronicle)

<parnas%QUCIS.BITNET@CORNELLC.CCS.CORNELL.EDU>
Thu, 7 Jul 88 12:42:50 EDT

One of the pleasures of not reading all the major U.S. papers is that I don't usually see articles that misquote me. The text by David Perlman that you cite is quite inaccurate. The first statement is a paraphrase of my words, not my words but my thoughts. I said that it was ludicrous to see people who are unable to tell a U.S. made F-14 from a French made Airbus, claiming that they will be able to write trustworthy software that will discriminate between Soviet warheads and Soviet decoys designed to look like warheads. The final quote in the article is not even an accurate paraphrase. I said that a system designed primarily as a defense against low flying high speed missiles should not be expected to discriminate between different kinds of aircraft. If the crew used a system in that way, i.e. if they assumed that the warning "threat" meant that the system "knew" it was tracking a military aircraft, then the crew made an error. I also told that reporter that we had far too little information to make any judgement on the failure of such systems. We do not know which data were used by the crew in making their decision. The Aegis missile defense software might not even have been involved.

Dave

Re: Iranian Airbus (RISKS-7.16) and the "facts"

Sue McPherson <munnari!murdu.oz.au!sue@uunet.UU.NET>
Fri, 8 Jul 88 15:14:23 EST

Over the last few days we've had a lot of emotional discussion about the shooting down of the Iranian Passenger Plane. All in all it has been about as informative as the discussions last year on KAL007 - that is - not very.

On the one had we have Hugh Miller who believes that the papers have told him that technology has fouled up again. On the other we have Michael Mauldin who thinks that the Captain made an understandable mistake and it was the Iranian's fault. Then there is Bob Estell who thinks his old buddy is one of the good guys so it must be the Iranians fault. But I can't help thinking that the Navy doesn't have such a good reputation these days for employing honest and reliable people. Finally we have Jim Anderson who thinks we should nuke the lot of them - er sorry, I mean shoot anyone within range.

Each of these people seems to be quite sure that they have the "facts" yet they seem to be quite contradictory. Just how trustworthy is the "Pittsburg Post" ? (who got it from the "New York Times" who got it from .....) It seems that we are very reliant on the media (newspapers & TV) yet we have no way of authenticating the information presented or even penalising them when they make a mistake. Interpretation of the "facts" is another risky area, a good example is the reported "fact" that the 707 has a cruising speed of 325 knots, while this may be the truth it is not the "whole truth" as there are other factors (such as wind speed) which could enable to the plane to travel at a much greater ground speed (i.e., the speed that would be observed by the US ship).

Both the "shootdown" and the ensuing discussions both prove the point that the biggest RISK we take, is in believing what we are told - whether the information comes from the latest/biggest/most expensive radar system or the "Pittsburg Post" there are no 100% guarantees that it is correct or even complete.

Sue McPherson sue@murdu.mu.oz

Threshold probability for declaring a radar blip "hostile"

Clifford Johnson <GA.CJJ@Forsythe.Stanford.EDU>
Thu, 7 Jul 88 00:54:41 PDT

I have a couple of observations re the Iran shootdown, and the big question, did Captain Will Rogers have sufficient cause to order it, as JCS Chairman Crowe loyally contends?

My first observation is that this claim seems premature, since no-one knows what information Will Rogers based his so-called decision (or should it be called computer-prompted reflex?) upon, as yet. Suffice it to say that if, as is reported, he did not bother to monitor to the air field control tower; and if, as is reported, Mode C (civilian) transponder returns were received by the ship; and if, as reported, the plane was flying at the speed of a commercial flight; and if, as reported, an F-14 is in any case no real threat to his ship; then on its face he was taking an unnecessary 50-50-ish gamble (not unreasonably characterized as a "panic") as to whether the radar blip was really hostile or innocent. Also, was it not negligent to not monitor the control tower, as is reportedly standard practice for non-U.S. ships in the Gulf?

But the question I really want to raise is, at what perceived "odds" -- 50-50,

60-40, 90-10 ? -- does a commander have "sufficient cause" to "declare" a radar blip, that might be hostile or might be a commercial flight, officially "hostile," so as to shoot it down? Judging by Admiral Crowe's immediate approbation, it seems he thinks that almost *any possibility* that a flight might be hostile is sufficient to order a shootdown, by virtue of the commander's "heavy obligation" to protect his "personnel and equipment." Judging by Will Rogers' simple explanation that he thought it was a hostile F-14, vague odds above 50-50 seem to be enough.

I would have thought that moral considerations would lead the military to value civilian lives above their own (isn't that what they are supposed to be guardians of?), and so the chances would have to be way *over* 50-50 to be sufficient to order a shootdown? Does anyone on the net think that odds of 51-49 or less are sufficient? A natural follow-on question is this: given the shortness of the response time, what could be the best odds attainable in a realistic attack scenario, even assuming the best computer technology the United States could field? Perhaps the degree of certainty simply cannot be high enough to justify a shootdown in any circumstances?

Iran Airline Incident and meaningful real-time data

Chris McDonald STEWS-SD 678-2814 <cmcdonal@wsmr10.ARPA>
Thu, 7 Jul 88 8:01:15 MDT

It seems to me that Martin Minow's comments on the danger of drawing conclusions in the absence of facts hits the mark. If I might pursue that line a little farther, I wonder if the Commander of the US ship was not forced to make a decision because he ultimately did not receive the most accurate or meaningful data. For example, neither the news media nor any official commentator has mentioned what data the AWACCS planes, which stage out of Saudia Arabia, did or did not see regarding the Iranian aircraft. From all published reports and publicity releases it seems likely--assuming that an AWACCS was airborne at the time of the incident--that the AWACCS detected the takeoff of the aircraft and may also have monitored signal communications between the aircraft and ground controllers. It also seems likely given the intelligence collection capabilities of several countries in the Gulf that other sources would have recorded the same information.

If these sources were available, then it seems logical to ask why one cannot discriminate between a fighter aircraft and a commercial airliner?

If these sources were not available, then it seems reasonable to ask why not?

A320 Airbus: Air conditioning; monitoring traffic control; F-14s

Steve Philipson <steve@aurora.arc.nasa.gov>
Wed, 6 Jul 88 21:00:43 PDT

Munnari!mulga.oz.au!lee@uunet.UU.NET (Lee Naish) asks:

> Though the A320 Airbus has redundant computer systems, they all use the

> same air conditioning system. Does anyone know what the expected
> failure rate of that system is, or how critical a failure would be?

Jet aircraft air conditioning is derived from the jet turbine's high pressure bleed air system and/or auxilary power unit. Air conditioning is thus available whenever an engine is running. If both engines fail, they may be able to use the APU in flight (some aircraft can only operate the APU on the ground), but this is probably not significant vis-a-vis instrument overheating, as the aircraft probably won't be flying long enough for the equipment to overheat. Computer system fans can fail, but there are usually several of these per machine and are not highly critical items.

minow%thundr.DEC@decwrl.dec.com (Martin Minow THUNDR::MINOW ML3-5/U26 223-9922) writes:

> that nobody on the Vincennes was monitoring tower-plane radio communications.
>(And the vague suspicion that there wasn't anyone on the ship fluent in Farsi.)

You don't really propose that every ship monitor every aviation and marine frequency within strike distance, do you? That would be at least dozens and perhaps hundreds of frequencies. Also it is very unlikely that tower transmissions would reach 20 miles away on the surface.

One should note the international language for air traffic control is English.

Jonathan Crone <CRONEJP%UREGINA1.BITNET@CORNELLC.CCS.CORNELL.EDU> writes:

> ... Grumman designed the F-14 to
> support the Navy's requirement for a powerful Air Defense Fighter.

> ... the F-14 has very limited Air to Ground capabilities...

> So perhaps the big question is, why are they saying that they
> were worried about the possibility of an attack from an F-14?

Iran wasn't supposed to have Silkworm missiles either. It must have really surprised the first few captains whose vessels were hit by them. Although the Iranians aren't exactly technical whizzards, it is possible that they could have configured an F-14 for air-to-surface operations. Would you risk your crew to save one belligerent opponent who has equipment of unknown capabilities?

Fred Arnold, a WWII P-38 pilot and author, noted that he always gave wide berth to Allied ships, as policy was that it was better to shoot down one friendly aircraft by mistake than to lose a ship. It seems that the policy is still in force today.

Iranian Airbus Blame?

<"chaz_heritage.WGC1RX"@Xerox.COM>
7 Jul 88 09:31:26 PDT (Thursday)

RISKS Digest 7.16 consists almost entirely of speculation and expressions of personal view about the shooting down of an Iranian civil airliner by the USS Vincennes.

Where are the hard facts? Where are the Flight Data Recorders? Where is the Cockpit Voice Recorder? Where is the data logger tape of the activity of the Aegis system aboard USS Vincennes at the time of the incident? When will the Log of the USS Vincennes be produced? Who will make known the Rules of Engagement under which the USS Vincennes engaged its target? Who drafted those Rules of Engagement? Which authority in Iran is reponsible for permitting the aircraft to fly through the area from a military base during a period of military action? Who in Iran is prepared to deny that the incident, tragic though it may be in human terms, is politically extremely convenient for Iran? Who in Iran is prepared to deny that fundamentalist Islam might well regard the 'martyrdom' of the Airbus passengers justified if it facilitates political victory over 'the Great Satan'?

It must be entirely unjust to assign blame to any party (or system) in the absence of admissible evidence. The fact that the unfortunate Captain of the USS Vincennes felt it necessary to make an immediate personal statement accepting full responsibility for the incident strongly suggests to me that he does not expect such evidence to be forthcoming. It is shameful that this officer, who has clearly done nothing but his duty, should have been placed in such an invidious position so soon after the incident in question.

Still more shameful is the clearly preprogrammed response of the broadcast media. We now have another addition to the 'Us and Them' Glossary:

USSR shoots down airliner = 'massacre'
USA shoots down airliner = 'tragedy'

Under such circumstances further Iranian political gain seems inevitable.

Chaz Heritage

Re: "The target is destroyed."

<mnetor!utzoo!henry@uunet.UU.NET>
Thu, 7 Jul 88 15:14:11 EDT

> "...So from now on it's hair-trigger 24 hours a day... Shoot first and
> ask questions later. The hell if I'm gonna be the next one to lose his
> Florida retirement condo to keep Marconi's rep clean." I can't find it in
> my heart to blame the man, either...

Nor can I, for a different reason. We're seeing yet another manifestation of the everything-should-be-absolutely-safe-and-if-it's-not-then-somebody-has-been-negligent syndrome. For heaven's sake, has everyone forgotten that (ignoring the political hairsplitting and sticking to the pragmatic facts

of the situation) there is a *WAR* underway in that airspace?!?

In a war zone, a bias toward shooting first and asking questions later is normal for anybody with any desire to survive. Wars are confused. The "to shoot or not to shoot" decision often has to be made with inadequate information. A "wait and see" decision is *very* hazardous to your health. "Own goals" -- shooting down your friends -- are normal in a war; the most one can do is try to reduce the frequency.

The fact is, when you take an airline flight through an area where a missile war is in progress, nobody in his right mind is going to expect that flight to be risk-free. You won't find me in an airliner anywhere near the Persian Gulf without an awfully good reason. Anyone who got on that flight as if it were a normal peacetime flight was either misinformed or crazy. Trying to be an innocent bystander to a war while standing in the middle of it is a damned risky project. The Stark incident evidently made the US warship captains aware of this. It's too bad the Iranian airline passengers had to learn the facts of life the hard way, but the people who fired those missiles cannot really be blamed for it.

Henry Spencer @ U of Toronto Zoology {ihnp4,decvax,uunet!mnetor}!utzoo!henry

---

An epilogue to this issue

Peter G. Neumann <neumann@csl.sri.com>
Fri, 8 Jul 88 15:42:11 PDT

For those of you who have waded through the past three issues of RISKS, I received MANY MORE contributions on this subject that have not been included here. This subject has generated a high level of interest, despite the lack of hard facts -- or perhaps precisely because of that lack. Yes, we should try to avoid rampant speculation, although it is important that we try to understand the conflicting factors in the absence of any definitive reports. (Several messages with rather wild rumors and speculations are omitted.) But the awaited ``definitive reports'' often turn out to be less than satisfactorily definitive (as in the case of the KAL 007). Difficult situations are in general not black and white, and the evidence is often not very precise -- if present at all.

I make no claims of infallibility. I sometimes err on the side of openness by including questionable material in RISKS. I prefer that to cloture. However, I think Gary's point at the top of this issue is very significant -- on the inherent difficulties in decoupling politics and technology, and indeed the dangers in trying to do so.

I sometimes also err by rejecting a contribution that deserves to be heard, but then I usually succumb to appeal. The Iranian Airbus incident has overwhelmed me with highly overlapping and speculative material. If one of your contributions overlaps one that is here, but still makes an important point still unsaid, please excerpt, rewrite, and resubmit.

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 18

Friday 8 July 1988

Contents

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

N-Version Programming

<jimv%omepd.intel.com@RELAY.CS.NET>
Thu, 07 Jul 88 18:04:34 PDT

Nancy, your mention of n-version programming in "Clarifications on the A320 Design" (recent RISKS) reminds me of an n-version failure I experienced last year.

In the design of the Intel's 80960 microprocessor, we generated two simulators for the instruction set. The first emulated the programs at the instruction level, and the second emulated programs at the logic/register-transfer level. These two simulators were developed independently from a detailed architecture specification. A third group wrote an automatic test generator, used for

validating the hardware and simulators, which created self-checking programs with "interesting" random operands and results.

All three implementations, both simulators and test generator, made the same mistake with the modulo instruction. The remainder instruction was implemented correctly, but the modulo instruction did an extra subtraction when the dividend and divisor had opposite signs and the dividend was an exact multiple of the divisor. (For example, 4 mod -4 returned 4, not 0.) The test generator tested for these cases, but wrongly computed the expected result in such a way that both the hardware logic and the test generator produced exactly the same results.

This mistake was discovered well after a year of software development on the processor by a user who was debugging an "impossible" condition.

Although this is the only explicit n-version failure we had, and even though the n-version approach found on the order of ten thousand design errors (estimated) over the course of the 5 year effort, this one failure was a striking experience. There were several more bugs that the n-version programming probably didn't find, but they're more forgivable because there even any tests generated for those sets of conditions.

For me, n-version programming is a valuable tool, but I wouldn't want to rely entirely on it.

Jim Valerio jimv%radix@omepd.intel.com, {verdix,omepd}!radix!jimv

---

Re: N-Version Programming [response to Jim Valerio]

Nancy Leveson <nancy@commerce.ICS.UCI.EDU>
Fri, 08 Jul 88 06:07:20 -0700

That is very interesting. It would, of course, also be interesting to determine whether the number of mistakes found by a different type of testing technique would have been less, as, or more effective. It is also possible that more "common mode" failures exist, but that noone has discovered them yet (the one you speak of was discovered, it sounds, by accident).

My student, Tim Shimeall, is just completing a dissertation in which one of the topics is a comparison of back-to-back testing (n-version testing) vs. regular testing. Eight versions of a specification were written independently and then the programs subjected to both back-to-back testing and regular testing. Even though the testers were undergraduate students and unskilled at testing (not something usually taught to undergrads), the back-to-back testing was not terribly effective in comparison to the other test methods used (structured walkthroughs, automated static analysis, functional testing). The problem is that voting is not a very good test oracle -- even on the same test cases, voting did not find the same errors as standard testing techniques. One of the reasons is that voting could compare final results only and not look at intermediate computations. Often, the testing methods that could thoroughly instrument a program detected errors that did not, for those particular input cases, actually result in wrong answers. Voting on intermediate results would

not have solved the problem. The errors did not exist at the abstract function level, but at a much finer level of granularity. Any attempts to vote at this level would have required that the specification include the exact algorithms and variables to be used, thus defeating the whole purpose of writing multiple versions and just moving the errors to the common specification.

We did find that the back-to-back testing detected errors that were not detected by testing. However, we cannot conclude much here because of the inexperience of the students doing the standard testing. We gave them a little instruction, but none had ever used these test methods before. This same type of comparison should perhaps be done with more experienced testers.

Almost all n-version experiments are either done in isolation (without comparing it to the alternatives in a controlled fashion) or have so many other methods applied to the programs in conjunction with the n-version programming that it is not possible to separate the effect of one method from the others. The important question is not whether one method of detecting errors finds some, but whether the alternatives that could have been used would have been better, the same, or worse at finding errors and whether they find the same errors or different ones (i.e., are alternative or complementary techniques). There are obviously costs associated with all these error-detection techniques and almost always a finite and limited amount of resources and time to apply them. The real question is how should these limited resources be spent.

No one has yet (including us) compared formal verification techniques with some of these other approaches. I just heard John Cullyer speak on the VIPER development and proof and was very impressed. My bias is to believe that formal techniques would be superior to many of these other techniques, but this needs to be confirmed using carefully controlled experimental comparison. In lieu of this, it will be interesting to see if the VIPER turns out to have fewer design and other errors than similar microprocessors developed using non-formal techniques.

The only small piece of evidence that I know of was obtained during an experiment by Brunelle and Eckhardt in which they had two more versions of the SIFT operating system (written at SRI using formal specification and verification techniques although not, in the end, completely verified to the code level) written by graduate students. When the three versions were run together as an n-version voting system, no errors were found in SIFT but there were instances of the two unverified versions outvoting the correct SIFT version. The programmers may, however, have had vastly different backgrounds and experience from the SRI programmer, so no real conclusions can be reached here. But it is interesting. Harlan Mills is also claiming very substantial gains from the use of formal development procedures on real projects at IBM.

Physical hazards

<mnetor!utzoo!henry@uunet.UU.NET>
Wed, 6 Jul 88 16:32:02 EDT

> CCI also cleverly placed the "reboot" switch, an up/down toggle, on the

> front of the cabinet, not recessed, and at knee level...

Some years ago, when I was with CSRI here, we had an analogous problem.
The machine room was relatively long and narrow, and we had two multi-
rack systems facing each other with consoles in the space in between.
The beat-up old swivel chair that we used as a console chair had a rubber
bumper strip high on its back so it wouldn't mar a wall (or whatever) if
you leaned back against one. Turned out that the bumper was at exactly the
height of the control switches on one of the RK05 disk drives. Oops...
We changed console chairs.

Henry Spencer @ U of Toronto Zoology {ihnp4,decvax,uunet!mnetor}!utzoo!henry

[This was not a case of "Chair and chair alike." PGN]

Accu-Scan inaccuracies

Robert Steven Glickstein <bobg+@andrew.cmu.edu>
Fri, 24 Jun 88 14:52:23 -0400 (EDT)

I once bought a little container of Minced Garlic at the Food Gallery on
Centre Ave., Shadyside. The shelf price was something like $1.89, I don't
really know. The scanned price, however, was $5287.44.

I was with a bunch of my friends, all of whom were very very amused by this.
Unfortunately, the checkout clerk and the manager were both fairly humorless,
and didn't appreciate our comments.

"Bad garlic crop this year?"
"Gee, I better really enjoy this garlic bread tonight."
"Do you take the American Express Gold Card?"
"Only fifty-two hundred? I'll take two."
"Reaganomics."
"Do you have change for a ten thousand?"
"Hmm. Garlic bread tonight, or a new car?"

-Bob Glickstein

Re: The Eyes Have It (RISKS DIGEST 7.16)

Don Watrous <watrous@aramis.rutgers.edu>
Wed, 6 Jul 88 21:04:52 EDT

All the original information for the last 5 digits of the NJ Drivers License
is correct (MMYYE) except for the omitted fact that 50 is added to the month
(MM) field for female drivers. I used to think that this was to make it a
less recognizable date (for women, who tend to conceal their age sometimes),
but now guess it's just adding in a coding for sex also.

I can confirm that all the Watrouses I know have the same initial letter and
4 digits. I'm curious as to how the middle 5 digits are arrived at.

Don

The Eyes Have It (Re: RISKS-7.14)

Evelyn C. Leeper <ecl@mtgzy.att.com>
6 Jul 88 13:34:45 GMT

[... also noted the +50 encoding...]

Even with all this, I have a driver's license that lists me as male! (Well, Mark and I both filed for a change of address on our licenses and I requested a change of name to add my middle initial, and they apparently added all the stuff together and sent me a temporary license with Mark's decsription!)

Evelyn C. Leeper 201-957-2070 UUCP: att!mtgzy!ecl or ecl@mtgzy.att.com

---

Re: Lockpicking, The Eyes Have It (RISKS-7.16)

<ames!desint!geoff@uunet>
Fri, 8 Jul 88 04:23:00 EDT

Randy D. Miller writes:

> If it's so easy to pick open locks, why do burglars resort to harder and
> messier ways of entering buildings, desks, cabinets, etc.? Are most burglars
> incapable of learning such a skill, or does it just not occur to them?

In the first place, the great majority of burglars are low-ambition, low-intelligence people. In general, they are looking for a quick, easy hit -- if they were interested in learning in a new skill, they'd most likely get a safer, higher-paying job. In the second place, why pick a lock when you can kick a door in, smash a window, or try the neighbor's house with the unlocked door?

In the same digest, Tracey Baker writes:

> It also makes me wonder about the NJ DMV...

I have a pretty low opinion of ANY organization that generates a supposedly-unique identification number from non-unique personal characteristics. What's wrong with assignments from a sequence, as with license plates and Social Security Numbers? The whole purpose is disambiguation; the current NJ system is, in a pithy analogy I heard yesterday, playing Russian Roulette using a clip-loading gun.

Geoff Kuenning geoff@ITcorp.com {uunet,trwrb}!desint!geoff

[Please let's not reiterate the many previous discussions on the use of an SSN. PGN]

re: lockpicking

Henry Schaffer <hes@uncecs.edu>
Thu, 7 Jul 88 15:55:09 edt

Randy Miller discussed the delights of lockpicking, and then raised some questions. He raised his chances of success by using inexpensive new locks. The lower the precision of the lock, the less the chance of quick picking. The BEST (brand) of locks is of standard construction (with regard to the pins and cylinder) but is very well made, and is quite difficult to pick. Then there are locks with specially designed pins (the Medeco brand is particularly well known) which make sucessful picking unlikely. Old/corroded locks are often difficult to work with.

Most of his questions also apply to physical security of computing facilities, and the concepts are even more general.

Most locks (e.g., in homes) are not extremely pick resistant, and there are perfectly good reasons why they are not. It is a principle of security that you should reinforce the weaknesses - and not waste time strengthening the already strong areas. (This also applies to computer security.) Since most (wood frame) doors, windows, desks, etc. are less resistant to force than their locks are to picking, it would be a waste of money to buy better quality locks. (This principle also applies to computer security.)

> I called some city and state offices, and one local locksmith, to see
>if there are any laws regulating the possession and use of lockpicks in
>Arizona. No one I talked to seemed to know anything about any regulations!

There is a "risk" of asking the wrong question! Ask again about possession of "burglar's tools"! (Yes, the definition of "burglar's tools" is context dependent.) It is not a good idea to have a lock pick in your pocket when you are in or around someplace which has been burglarized!

> If it's so easy to pick open locks, why do burglars resort to harder and
>messier ways of entering buildings, desks, cabinets, etc.? Are most burglars
>incapable of learning such a skill, or does it just not occur to them?

It isn't so easy (you, a technical person, spent quite a bit of time learning/practicing this.) A 2' crowbar or strong screwdriver will usually work faster, and with less practice needed - and who cares about "messier"?

>Should I spend a fortune replacing the locks on my house, or are the risks
>low that a burglar will pick the locks?

If the easiest way to get into your house is by picking the lock(s), then you probably should replace them. Spring latch locks can also be defeated by use of a piece of flexible plastic or metal - do you have dead bolts?

--henry schaffer n c state univ

Lockpicking (Re: RISKS-7.16)

Lee Hounshell <tlh@pbhyf.PacBell.COM>
7 Jul 88 16:33:13 GMT

>[Randy D. Miller writes..
> If it's so easy to pick open locks, why do burglars resort to harder and
>messier ways of entering buildings, desks, cabinets, etc.? Are most burglars
>incapable of learning such a skill, or does it just not occur to them?
>Should I spend a fortune replacing the locks on my house, or are the risks
>low that a burglar will pick the locks?]

Picking a lock takes time, and sometimes even locksmiths can't do it quickly.
I remember being locked out of a condo at Lake Tahoe last year, and the
locksmith who was called out to open the place up spent 2 hours trying to
pick the lock. Finally, he gave up and took out a hammer and chisel. Just
two hits on the deadbolt were all that was needed to completely demolish it.
The door was open in about 10 seconds. What really amazed me was how quickly
anyone can get into someone's home, just with a hammer and chisel. Locks
only keep out honest people.

Lee Hounshell

Another "silent fault tolerance" example: DWIM

<obrien@aerospace.aero.org>
Fri, 01 Jul 88 12:50:43 -0700

I can provide a more modern example of "too silent" error
recovery. A couple of years ago I was programming in Berkeley Smalltalk:
the implementation of Smalltalk on a Sun. I was surprised at how slow
the graphics of the system was, and went in to tweak the virtual machine.
First, I "batched" the bitmap operations.

Nothing happened.

I put in a few print statements to see what was going on in there.

Nothing happened.

In desperation I put print statements all over the place.

Finally, something happened - but not much. The virtual machine
operation was returning an error immediately (this was "drawLoopXY" for
the curious). Interpreted Smalltalk code was then taking control and
doing the drawing using more primitive calls. In all its history,
Berkeley Smalltalk virtual machine had never actually drawn any lines!
The Smalltalk code was silently doing it all, at far less speed.

I had thought this experience unique, until I saw the message
about DWIM. I wonder how many of our "high-level programming environments"
are running much, much more slowly than they need to?

Mike O'Brien
The Aerospace Corporation

ATM receipts

Joe Beckenbach <beckenba@csvax.caltech.edu>
Tue, 5 Jul 88 23:23:15 PDT

One of the RISKS readers wrote in to register his surprise at the concept of receipts for withdrawals and also for deposits, taking the more traditional legal "exchange money for receipt" view.

The ATMs here in Los Angelos give "receipts" for deposits, withdrawals, transfers, and user-selected balance checks. The receipt for deposits is the traditional legal-style notice that money has been received. The "receipt" for the other transactions are hard-copy of the transaction, and therefore not a receipt in the strictest sense. For instance, I find it very worthwhile keepng the withdrawal 'receipts' from my checking account ATM withdrawals: balanced checkbooks are happy checkbooks. Hardcopy balance statements are handy for trying to figure out when checks cleared to contest a bounced check, and an ATM transfer of funds needs a record just as much as any other deposit does.

And a deposit accepted without a receipt is a donation. No joking. Even most organized charities give receipts for donations accepted.

Rather "receipts" than mute ATMs! Joe Beckenbach

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 19

Sunday 10 July 1988

Contents

- Iranian Airbus discussion
  - Philip E. Agre
  - Tracy Tims
  - Hugh Miller
- Info on RISKS (comp.risks)

Iranian Airbus discussion

Philip E. Agre <Agre@WHEATIES.AI.MIT.EDU>
Sat, 9 Jul 88 18:24 EDT

An interesting analogy connects a number of the disagreements over topics like the shooting of the Iranian airliner. Some people want to stick to the technical details and leave politics out of it; others reply that the distinction is untenable since politics is part of the reality in which products of technology operate. Likewise, some people want to discuss the conduct of war as if it occurred in a reality free of politics. The latter was once possible but now it isn't. But why? Roughly speaking, because the world is a smaller place. For one thing, the efficiency of modern communications media make it possible to conduct a `political war'. For another thing, great increases in the velocities and ranges of both weapons and civilian transportation make it much harder for civilian activities to stay out of the way of `war zones'. Yet the model of `pure war' continues to inform the design of most computerized weapons systems. All of the doctrines, indeed all the vocabulary, of Western warfare were developed in the context of such well-defined, all-out wars as the major modern European wars. These wars started and ended at definite times, opposed clearly defined alliances in which all relevant parties felt the need of choosing sides, and were conducted by militaries whose only political constraint was the necessity of winning. Everyone understood that civilian life simply came to a complete halt during these wars. These episodes serve as our prototypes of a `war', a category about which one makes generalizations by consulting a historiography of warfare, written by modern Westerners, that concentrates on episodes that fit this

pattern. The concept of `civilian' is simply the flip side of the concept of `war'. This concept of warfare is just as much a part of the models implemented by the computers on the Vincennes as the concepts of physics used to describe signals, trajectories, and explosions. As we well know, when the models underlying a computer system are wrong, the computer will make mistakes. Most of the systematic organized violent conflicts in the world today are not `pure wars' but rather drawn-out low-level conflicts in which the smallest details of military operations are political actions organized by political considerations. The inappropriateness of the `pure war' model explains many recurring themes in interviews, long before the Iran Air incident, with the military people running the US operations in the Gulf, both the sailors on the ships and the admirals back in Washington. They complain bitterly, for example, of having to ``fight a war in a lake'' and of the narrow margins placed on their decisions by the presence of non-military planes and boats, many of which (especially the boats) do not own or competently operate the radio systems that permit ready discrimination in peacetime traffic control. Thus the naval battle that was occurring at the precise moment when the Air Iran plane approached the `war zone' was not at all a prerequisite for such an incident. The ultimate questions are: As warfare and politics blur, what should be call what's happening in the Gulf (and two dozen other places in the world) if not a `war'? And then, as technical practice and politics blur, what should we call what happens in laboratories and factories if not `technology'?

Responsibility (Iranian Airbus)

Tracy Tims <ttims%watdcsu.waterloo.edu@RELAY.CS.NET>
Sat, 9 Jul 88 18:52:39 EDT

It is true (as Henry Spencer points out) that you would have to be "misinformed or crazy" get on that flight as if it were a normal peacetime flight. On the other hand, the fact that we do not judge such people wise should not affect the way we judge those who caused their deaths.

If a woman takes a risk (say, walking home from work through a suspect neighborhood) that leads to her being raped, we may question her judgement in taking the risk, but we in no way reduce the burden of responsibility on the man who actually did the raping. We may suggest that she avoid walking in the area, but we know that it is not right to expect women to limit their lives because of a danger some criminals have decided to threaten them with. The desired situation (in fact the moral situation) would be no risk to women of rape. There would have been no risk of rape (and no rape) had not some man decided to create one. One must not fall into the trap of transferring responsibility from the perpetrator onto the victim.

Likewise, there would be no real risk of an airliner being shot down by a missile had not some group of people decided to create that risk. Yes, we can question the judgement of a group of people who decide to expose themselves to that risk, but we cannot lessen the moral responsibility of the people who created the risk and who performed the action.

By having a shoot-first-ask-questions-later policy, in a zone where both military and peacetime activities co-exist (and, as I'm sure we all agree, where only peacetime activities should be), a military that is executing policy places the risk of executing that policy squarely on the shoulders of potentially innocent people. Given the fact the the U.S. chose to conduct military operations where there were innocent bystanders I feel strongly that they should also be willing to accept any attendant risks. Anything less than that amounts to sticking other people with the bad results of their decisions. The Navy has a moral obligation to decide whether or not a blip on their screen is an attacking aircraft and not an airliner, if there is a significant chance that it could be an airliner. If they cannot, they should not place the risk of misidentification on some innocent passengers. I feel this especially in this case, where the U.S. Navy is not fighting a war for U.S. survival against unprovoked attack, but is implementing a peacetime foreign policy decision.

> It's too bad the Iranian airline passengers had to learn the facts of life the hard way, but the people who fired those missiles cannot really be blamed for it.
> - Henry Spencer

I think this statement has a profound lack of empathy, but I find the last part of it, "the people who fired those missiles cannot really be blamed for it," to be completely absurd and dangerous. Any atrocity can be justified using very similar words: "it's too bad she had to learn the facts of life the hard way, but the man who raped her cannot really be blamed for it." (After all, she really caused the crime, by placing herself in the position where it could happen, right?)

The people who died in the airliner did not kill themselves. Captain Rogers killed them. A sidereal examination of the facts of the incident shows this clearly. At most, the passengers are guilty of stupidity, optimism and bad judgement. Captain Rogers is guilty of their deaths.

The problem with man-made risks in general is not so much detecting them, but trying to find someone or some group to actually be responsible for them. If the responsibility for a risk (and its consequences) is diffuse, or state sanctioned, or complicated by the fact that the victims apparently chose to accept the risk; then people are all to quick to deny any blame. This is a moral failing. Many technological risks (from the design of user interfaces to the existence of nuclear weapons) are orphans in this sense.

Tracy William Lewis Tims

The Iranian Airbus and following discussion

Hugh Miller <HUGH%UTORONTO.BITNET@CORNELLC.CCS.CORNELL.EDU>
Sun, 10 Jul 88 09:56:53 EDT

I've had _numerous_ private messages & some RISKS postings responding to my submission to RISKS 7.15 ("The target is destroyed"). A few warranted replies, so I have tried to draw up same here. (I have not responded to Gary Chapman's posting in RISKS 7.17, since I agree emphatically with everything he

says.)

(1) Michael Mauldin (RISKS 7.15) taxes me with getting the facts wrong. I plead guilty. If you note the header of my message you will see that it was -- well, 'fired off' I guess is the right phrase -- at 11:15 on Mon 04 July, at which time even the most elementary facts were in dispute. For that matter, several of the 'facts' Mr Mauldin and others report have since been, uh, revised. My main points, however, rely (I hope) less on facts than on possibilities. I would be tempted to call them 'philosophical' did that not open them to the usual (and deserved) snorts of derision 'hard science' types reserve for contemporary so-called 'philosophy.'

Similarly, Sue McPherson charges from Down Under "that the papers have told him that technology has fouled up again." I can assure her that I never believe what the papers tell me. I grew up in Louisiana. As for technology doing what it ought in this case, well, 290 dead civilians indicates otherwise to ME. Her words radiate the confidence of technolatry: if we can get the facts straight & keep the media & the pols out of the control room we can fix this sucker right now so it'll never happen again. But whether, in this instance, Capt Rogers made the 'right' call or not, whether the EW gear 'worked' or not, we still have to ask some very fundamental questions about technology.

Let's not be under any illusions about whether we will ever get the "real facts," the nitty-gritty technical details, of the Flight 655 tragedy. (Perhaps 12 months from now one of you reading this will get hired by the Pentagon to write some code for the AEGIS system to prevent such-and-such a, purely hypothetical you understand, 'problem' from occurring. I would like to think you would do the right thing and tell us, but doubtless you will be sworn to infinite secrecy.) In Montreal, where I used to live, complaints against the Police de la Communaute Urbaine de Montreal were investigated by -- the Police de la Communaute Urbaine de Montreal. Needless to say, such complaints were unexceptionally dismissed as groundless. With the stakes stupendously higher, what reason have we to believe that the US government (to say nothing of our lickspittle press) will behave in any less self-serving a fashion? 290 dead innocent airline passengers, 66 children among them, is, to put it crudely, one hell of a spin-control problem.

(2) Bob Estell (RISKS 7.15) knew Capt Will Rogers before the Navy & finds it hard to believe he (Rogers) would have behaved in any other way save the honorable. Given the alternative, I hope for Capt Rogers's sake he is right. But military training of any sort changes a person, in my thin experience in the matter; it is intended to; and the results are for the 'good' only when that 'good' is evalued from the standpoint of the profession of arms. At any rate, Capt Rogers either made a bad judgment on the basis of good evidence, a good judgment on the basis of bad evidence, or a bad judgment on the basis of bad evidence. I cannot bring myself to believe Capt Rogers, any more than Capt Brindel before him, was capable of the first, and I hope none of us can. (That may not keep him from being scapegoated.) If versions 2 or 3 are correct, then the particular technology, to quote George Bush, is "in deep doodoo." And in any event technology

in the broadest sense is what gave us the "Roger-willco" attitude that got us embroiled in this hellacious war in the first place.

(3) Jim Anderson (RISKS 7.16) faults Iran Air for its imprudence, at best, in sending a commercial airliner over a combat-engaged US AEGIS cruiser. IF indeed the facts are as my government represents them (I am, by the way, a native-born US citizen and a landed immigrant in Canada), then I might fault the people at Iran Air for poor judgment; perhaps I might even go so far as to hold them technically liable at law for criminal negligence indirectly causing death. As to the true facts of the engagement, well, as of today (9 July) the US has, ahem, changed its story a few times. As a highly interested party its account will always be suspect. But even if the facts are as we represent them, since the US is not officially at war with Iran (at least as far as Congress, which under the Constitution has the exclusive power to declare war, is concerned) we had and have no right to be where we are in the first place, under strict interpretation of international law and maritime convention, to say nothing of good old practical political reasoning. (Henry Spencer, RISKS 7.17, please take note. This is not 'our' war.) Let me pose the following 'scenario', as the gamers say: suppose you are a citizen of, say, France, in the year 2000. Margaret Thatcher, now in her 18th term of office, declares war on your country. The USSR, for 10 years thanks to _perestroika_ engorged on Western high technology and a big consumer of oil from the North Sea, decides to protect its supply by sending in a huge naval tactical group, some of which stays outside the North Sea & English Channel, but much of which goes in to reflag tankers with the Soviet standard & generally harass & fire on French vessels while ignoring English ships. In short order their EW technology, still at US 1988 levels, leads them to shoot down an Airbus A920. The Soviets say the French were to blame; some Russians claim fanatical French deconstructionists had sent the airliner on a deliberate kamikaze mission, or had tucked a MiG-99 behind it, or AT BEST just should have known better than to tempt the wrath of the Bear. Describe your feelings, as a French citizen. (For fun, imagine what the Pentagon would be thinking.) This was my point: we are in the the Gulf only partly because of greed and the normal, predictable imperialist tendencies we have exhibited for over a century. REAL prudence would counsel us not to be there, and statesmen of an earlier day would probably have heeded that counsel. But the Mephistopheles of technology, to whom we have sold our soul, remember, whispers: "We _can_ do it. If we _can_ do it, we _should_ do it. If we _should_ do it, we _must_ do it." Technology is much more than just a tool. It is a world, a universe of discourse, a mythology (as PGN put it elsewhere in the issue), a devil of a weirdly affectless sort, but persuasive as any tempter. He has entered into us like the demon into the Gadarene swine, and driven us headlong, not this time into the Sea of Galilee, but into the Persian Gulf.

Mr Anderson's final point is thus the most disturbing, the more so for its offhanded, sensible flavor. "Let's get the forum back to technical risks," he urges, "and off of the political beat." Again, this is my point: the two are as inseparable as the faces of

> Janus. The flashpoint of their union is the armed forces of the US and NATO, and to a much lesser extent those of the Soviet Union, the Warsaw Pact, and other nations. Technology, or rather its apologists, dissembles this; part of the hoodwink consists in its claiming to be just a means, completely separate from any consideration of ends. We are more than happy to go along, to let ourselves be deceived, for the sake of the lovely, tangible, short-term amenities and conveniences it supplies. (Anyone who has doubts about America's capacity for self-deception must have been on Mars for the past 8 years.) Technology is, rather, for us, an end in itself as well as the means thereto, THE end-in-itself _par excellence_. (The end, PERIOD, I'm tempted to say.) This, to my mind, is where a more fundamental consideration of the "RISKS" posed by technology must begin.
>
> Such a reconsideration, it seems to me, would have to go far beyond the received wisdom. It would have to question what we take completely for granted, and when one does this one always runs the risk of being deemed insane, reactionary, or Luddite, no matter how much one loves one's children & the future. Is, for instance, the entire modern project of unlimited progress through the conquest of nature, of which technology is the articulation, the Unqualified Good we assume it to be? The project of the conquest of nature seems itself founded upon still deeper assumptions, such as the mechanical character of human and nonhuman nature, the total freedom of human cognition and valuation, the denial of transcendence, etc. But the most important such assumption seems to be that compassion for the lot of one's suffering fellow human beings must override all other practical and theoretical considerations. In Feuerbach's words, "compassion must precede thought." Are we prepared, in the light of the chaos into which our 'compassionate' and 'thoughtful' technology is about to precipitate us, to rethink even these assumptions?
>
> Turning back to bits and bytes (permanently) is tuning out to the deeper issues. I can play with the details as well as anybody, I suppose, but just as in a corporation you'll never get promoted to CEO if all you want to do is sit at a terminal all day and code, so we cannot be free men and women, "The People" to whom our Constitution makes constant reference, if we do not undertake to THINK about What Gives Here Anyway?

If I may be permitted a personal point, at the risk of making this sound like some maudlin Lance Morrow "Time Essay": Someone may object, "Well, for an anti-technologist you seem to have no problems with the computer, the pre-eminent technology." All right. But with me the issue of technology is much more painful to think through than whether or not I am prepared to go back to the typewriter or even the quill pen. My adorable one-year-old recently underwent a balloon valvoplasty for a blocked heart valve. Without the operation the prognosis was death by heart attack or congestive heart failure by six months of age. Today he is well and will lead an utterly normal life, provided he does not fly on an Iranian airliner near an AEGIS ship. For me, to think about technology at a fundamental level means to come face to face with the bitter possibility of my own son's certain death. Unless we are prepared to think at that level we will go on killing, puzzled, wishing we didn't have to, but hopelessly going on and on. The great English poet Stevie Smith, writing about theology in her poem "How Do You See?" has

words that the priests and priestesses of the new religion of technology would do well to heed:

> I do not think we shall be able to bear much longer the dishonesty
> Of clinging for comfort to beliefs we do not believe in,
> For comfort, and to be comfortably free of the fear
> Of diminishing good, as if truth were a convenience.
> I think if we do not learn quickly, and learn to teach children,
> To be good without enchantment, without the help
> Of beautiful painted fairy stories pretending to be true,
> Then I think it will be too much for us, the dishonesty,
> And, armed as we are now, we shall kill everybody,
> It will be too much for us, we shall kill everybody.

Questioning technology as profoundly as we must is so painful and vertiginous I doubt we can do it. I hope we can; but I doubt it.

That's all for now.

Hugh Miller University of Toronto (416)536-4441 <HUGH@UTORONTO.BITNET>

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 20

Monday 11 July 1988

Contents

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

"Computers may be at root of jet downing"

Peter G. Neumann <NEUMANN@csl.sri.com>
Mon 11 Jul 88 10:34:52-PDT

From the Washington Post, on the front page of the San Jose Mercury News,
11 July 1988:

WASHINGTON -- Computer-generated mistakes abourd the USS Vincennes may lie at the root oooof the downing of Iran Air Flight 655 last week, according to senior military officials being briefed on the disaster.

If this is the case, it raises the possibility that the 290 Iranian passwngers and crew may have been the first known victims of "artificial

intelligence," the technique of letting machines go beyond monitoring to actually making deductions and recommendations to humans.

The cruiser's high-tech radar system, receivers and computers -- known as the Aegis battle management system -- not only can tell the skipper what is out there in the sky or water beyond his eyesight but also can deduce for him whether the unseen object is friend or foe and say so in words displayed on a console.

This time, said the military officials, the computers' programming could not deal with the ambiguities of the airliner flight and made the wrong deduction, reached the wrong conclusion and recommended the wrong solution to the skipper of the Vincennes, Capt. Will Rogers III.

The officials said Rogers believed the machines -- which wrongly identified the approaching plane as hostile -- and fired two missiles at the passenger plane, knocking it out of the sky over the Strait of Hormuz. [...]

System `flawed' in tests

On the question of the Vincennes' performance, Rep. Denny Smith, R-Ore., a longtime critic of the Aegis program, said Sunday on the ABC News program "This Week With David Brinkley" that the type of phased-array radar system carried on the Vincennes has proved "flawed almost every time" in a recent series of Navy tests. [...]

Military officers with combat experience stopped short of criticizing Rogers for firing but said a skipper who relied more on human intelligence than artificial intelligence might have doubted that the approaching plane was an Iranian F-14 intent on attacking his ship for these reasons:

/ The approaching plane had not focused either its search or fire-control radar system on the Vincennes and had identified itself at least once electronically as an airliner as well as an F-14, an air-to-air fighter that Iran has not used against ships.

/ The plane was descending from a high altitude, between 9,000 and 12,000 feet, making it vulnerable to the Vincennes' missiles and guns. Rogers had about four minutes -- enough time to handle a single threat -- to shoot the Airbus down after it came within sight but before a hostile plane could use its cannons or drop unguided bombs accurately.

(The Iranian F-14 is not wired for anti-ship missiles, which would be dropped during a different flight profile than the Airbus was flying, and has not shown the ability to use laser-guided bombs in such a single-airplane attack.

/ A single plane would be unlikely to attempt a kamikaze attack against such a heavily armed and highly maneuverable ship as the Vincennes.

Newspaper disputes account

The Pentagon's account of the incident came under fire from a new direction Sunday when the Sunday Times of London reported that the British Government Communications Headquarters had determined from electronic eavesdropping that the Iranian Airbus left Bandar Abbas only three minutes behind schedule, was flying in the correct flight path south over the Strait of Hormuz toward Dubai in the United Arab Emirates and was climbing when the Vincennes shot it down.

Adm. William J. Crowe Jr., chairman of the Joint Chiefs of Staff, said July 3 that the Airbus was outside the commercial corridor, an assertion the Pentagon stepped away from Thursday, and was descending toward the ship in an

attack mode. The Pentagon has said the airliner was 27 minutes late taking off.

The newspaper said that the communications headquarters report was "severely critical" of the U.S. Navy for shooting down the Airbus and suggests that the initial confrontation between the Vincennes and three Iranian gunboats may have been provoked by U.S. helicopters flying into Iranian airspace. The Pentagon has said a helicopter from the Vincennes was fired on by the gunboats, triggering return fire from the cruiser. Pentagon officials declined to comment on the Times report.

Iran Airbus tragedy

<cdsm%DOC.IC.AC.UK@CUNYVM.CUNY.EDU>
Mon, 11 Jul 88 15:22:43 BST

[...] Some people writing in the US may not realise that Dubai airport, to which the flight was heading, is the busiest transit point in the region. It would change a LOT of schedules if it were closed.

Chris Moss

Shooting down Flight 655

<LIN@XX.LCS.MIT.EDU>
Mon, 11 Jul 1988 00:47 EDT

I've just read the last few issues of commentary about this subject, and I find the debate sadly misdirected. The one really relevant comment came from Gary Chapman, who says we should not look at just the technical issues.

The point is not to learn why the Vincennes was unable to identify a civilian airliner as such. The US military has known for 20 years that the IFF problem (Identification Friend or Foe) is a VERY tough problem, and no good solutions exist as yet, other than visual identification. If you send ships into areas in which weapons will be fired at other things in the area, sooner or later an innocent target will be destroyed. We can argue till the cows come home the precise nature of this particular error, but in the larger scheme of things, it really doesn't matter. Whatever this reason is, the next time it will be some other reason.

The real issue -- if you are determined to save innocent lives -- is why the US Navy is in the Gulf at all. The only sure way to make sure you don't -- at some point -- have innocent blood on your hands is to not send your weapons of war into an area where they could be used. The technology doesn't matter; the policy does.

On the other hand, maybe RISKS isn't the right place for a strictly policy debate. Try ARMS-D for that, maybe?

Herb (ARMS-D moderator)

Ignoring the wolf

Andy Freeman <andy@polya.Stanford.EDU>
Fri, 8 Jul 88 23:03:45 PDT

The July 8 issue of the San Francisco Chronicle had an article by Karen DeYoung of the Washington Post. She reported on a news conference by Brigadier General Mansour Satary, "the chief of Iran's Air Force." The last paragraph of the article was:

"Asked why the airbus failed to respond to what the Pentagon has said were 12 separate radio queries, on both military and civilian frequencies, to identify itself, Satary said that such communications from the American ships in the gulf were so frequent that Iranian pilots usually ignored them."

-andy

Air France Airbus crash

<mnetor!utzoo!henry@uunet.UU.NET>
Sun, 10 Jul 88 21:57:41 EDT

> Does the Airbus model in question display altitude in feet or meters?
[Question raised regarding whether the Air France Airbus was at 30 feet or 30 meters...]

Unless I am greatly mistaken, in feet. Altitudes and airspeeds are not quite the same situation as fuel volumes. The latter are a matter for individual aircraft; the former are of vital interest to air traffic control and other aircraft, and units are internationally standardized (altitude in feet, airspeed in knots). I wouldn't even expect readouts in both units, because altitude and airspeed are safety-critical items and even the slightest confusion about which number is which is unacceptable.

It's kind of unfortunate that aviation standardized on units that are now obsolete, but this is one of those cases where the actual units are not very important so long as they're standard. For navigation one needs to turn airspeed into map distance, and for the initial phase of takeoff and the final phase of landing the absolute altitude is significant, but otherwise comparisons are usually relative and the units of measurement don't matter much. For example, what matters about airspeed is not its absolute value, but its value relative to safe limits, optimal values for the particular phase of flight, and the value requested by traffic control. Even near-ground altitudes are relative to some degree: 50 feet of altitude is a good takeoff-obstacle clearance for a Cessna, a dangerously small one for a 747 (which can't do a hard turn without sticking a wing down farther than that), and a routine operating altitude for military aircraft in wartime.

Henry Spencer at U of Toronto Zoology
uunet!mnetor!utzoo! henry @zoo.toronto.edu

Re: Physical hazards - poorly designed switches

John Robert LoVerso <loverso%encore@multimax.ARPA>
Mon, 11 Jul 88 16:01:50 EDT

Dave Curry relates of some problems with a CCI Power 6/32:
> CCI also cleverly placed the "reboot" switch, an up/down toggle, on the
> front of the cabinet, not recessed, and at knee level. Fortunately,
> UNIX seems to ignore the switch.

At SUNY/Buffalo, the Sperry 7000/40 there that I had running 4.3BSD-tahoe beta did respond to that switch (I remember leaning over the front of the processor once, only to end up rebooting it).

That machine suffered my worst abuse. To the left of the front reboot switch was the key switch for local/locked/off. I once knocked into it, only to break the end off of the key.

CCI also used a clever placement strategy with the "emergency shutoff" switch, a large red push button. This was on the back of the cabinet, extending out 1" at waist level. Pressing this would trip the main breaker for the CPU and disks. It was easy to lean on this button and then suddenly notice the quiet in your end of the machine room. Unfortunately, this machine was far from the VAXen in the room, and behind it was one of the quieter locales in the machine room, so I frequently stood in that area while talking to people. And, more than once, I accidentally hit that switch.

One day, I was imparting upon the field service tech how poorly designed this switch was (and he was telling me how it was required by law to have an easily accessible emergency cutoff?!) when I (accidentally) leaned on darned thing again.

The very next day I took the mounting bracket apart and replaced it in such a way that the switch was recessed 1" into the cabinet. Never again did I hit it accidentally.

Henry Spencer tells of a chair that liked RK05s. I was told a story about CU/Boulder, where they used to use munchkins (12 year olds) to do dumps. They had the familiar RA81/TU80 combinations common to VAX 11/750s, where the RA81 controls are about 18" from the ground. One particular short munchkin had the problem of repeatedly off-lining the drive while mounting the tape to dump it. As with Henry's chair, he was replaced by someone taller.

John R LoVerso, Encore Computer Corp

PIN on PNB calling card

Mark Mandel <Mandel@BCO-MULTICS.ARPA>
Mon, 11 Jul 88 09:26 EDT

Scott Peterson's reaction to Pacific Northwest Bell's encoding his calling card PIN in the magstripe is simply to "hit [his] card with a bulk tape eraser, and forget about using card reader phones until PNB straightens this out". Scott, have *you* called PNB's attention to this monumental piece of stupidity? Has anyone? Or do you trust the same crew that implemented this un-security measure to realize their mistake unaided and take the initiative to correct it? "Marketing sez the customers want the convenience, and they haven't gotten any complaints, so if it ain't broke [i.e., not causing us any grief] don't fix it."

-- Mark Mandel

Re: Lockpicking

<mnetor!utzoo!henry@uunet.UU.NET>
Sat, 9 Jul 88 23:45:42 EDT

> Should I spend a fortune replacing the locks on my house, or are the risks
> low that a burglar will pick the locks?

A local insurance outfit might be able to tell you what the incidence of such things is locally. Do beware of one complication: since picking leaves no major physical traces, it is a convenient scapegoat for cases where the *real* problem was the owner's carelessness. Orthodox wisdom is that most "burglar picked the lock" cases are really "burglar had a key" or "door was not locked".

My understanding is that picking is perceived as difficult and possession of lockpicks (aka "burglary tools") is perceived as too likely to be incriminating. I would be surprised if Arizona didn't have a possession-of-burglary-tools law; before spending a fortune on locks, spend a little asking a lawyer about this. (Local officials are notorious for being uninformed about the laws they are supposed to enforce, so I wouldn't put too much faith in the negative results you got by asking them.)

Henry Spencer @ U of Toronto Zoology {ihnp4,decvax,uunet!mnetor}!utzoo!henry

---

lockpicking

Robert Mathiesen <SL500000%BROWNVM.BITNET@MITVMA.MIT.EDU>
Mon, 11 Jul 88 08:37:45 EDT

Apropos of Randy D. Miller's surprise that information on lockpicking is so readily available, I cannot resist quoting Charles Tomlinson's Rudimentary Treatise on the Construction of Locks, published about 140 years ago. His words are also relevant to much of the discussion on computer security which has gone on in this Forum.

"A commercial, and in some respects a social, doubt has been started within the last year or two, whether or not it is right to discuss so openly the security or insecurity of locks. Many well-meaning persons suppose that the discussion respecting the means for baffling the supposed safety of locks offers a premium for dishonesty, by showing others how to be dishonest. This is a fallacy. Rogues are very keen in their profession, and already know much more than we can teach them respecting their several kinds of roguery. Rogues knew a good deal about lockpicking long before locksmiths discussed it among themselves, as they have lately done. If a lock -- let it have been made in whatever country, or by whatever maker -- is not so inviolable as it has hitherto been deemed to be, surely it is in the interest of *honest* persons to know this fact, because the *dishonest* are tolerably certain to be the first to apply the knowledge practically; and the spread of knowledge is necessary to give fair play to those who might suffer by ignorance. It cannot be too earnestly urged, that an acquaintance with real facts will, in the end, be better for all parties. Some time ago, when the reading public was alarmed at being told how London milk is adulterated, timid persons deprecated the exposure, on the plea that it would give istructions in the art of adulterating milk; a vain fear -- milkmen knew all about it before, whether they practised it or not; and the exposure only taught purchasers the necessity of a little scrutiny and caution, leaving them to obey this necessity or not, as they pleased. ..... The unscrupulous have the command of much of this kind of knowledge without our aid; and there is moral and commercial justice in placing on their guard those who might possibly suffer therefrom. We employ these stray expressions concerning adulteration, debasement, roguery, and so forth, simply as a mode of illustrating a principle -- the advantage of publicity. In respect to lock-making, there can scarcely be such a thing as dishonesty of intention: the inventor produces a lock which he honestly thinks will possess such and such qualities; and he declares his belief to the world. If others differ from him in opinion concerning those qualities, it is open to them to say so; and the discussion, truthfully conducted, must lead to public advantage: the discussion stimulates curiosity, and curiosity stimulates invention. Nothing but a partial and limited view of the question could lead to the opinion that harm can result: if there be harm, it will be much more than counterbalanced by good."

The subsequent development of lockmaking in the course of the next 140 years has long since demonstrated the correctness of Tomlinson's argument in his own field. I do not doubt that it is equally applicable in the area of computer security.

---

re: lockpicking and burglars

Doug Faunt (phone (415) 496-4727) <faunt@spar.slb.com>
Fri, 8 Jul 88 22:44:02 PDT

I would like to point out that it might be worthwhile to improve your locks to some degree, since an intruder who picked the lock probably wouldn't leave any evidence of the intrusion, and at least one of my insurance policies DOES NOT cover, "mysterious disappearance". You may not be able to keep them out, but you can make sure there's a record. This has obvious applicability to computer security measures.

...{amdahl|decwrl|hplabs}!spar!faunt faunt@spar.slb.com

Lockpicking

<"chaz_heritage.WGC1RX"@Xerox.COM>
7 Jul 88 09:31:26 PDT (Thursday)

In his Tue, 5 Jul 88 09:44:06 MST Randy D. Miller writes:

>I called some city and state offices, and one local locksmith, to see
if there are any laws regulating the possession and use of lockpicks in
Arizona. No one I talked to seemed to know anything about any regulations!<

I feel that I ought to ask the Phoenix, Arizona Police Department how they would feel about searching Mr. Miller's home for >$0.99 hacksaw blades and a Dremel Tool grinder<.

Exactly this 'ban it all' attitude is very prevalent in UK. If someone is murdered with a knife, the media howl for all knives to be 'banned'. What they should howl about is that someone is motivated to murder - not that someone who was so motivated chose a particular instrument.

Or perhaps Mr. Miller would be happy to live under a law that prohibited possession of lockpicks - or the means to make them - or the knowledge of how to make them.....

Chaz Heritage

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 21

Tuesday 12 July 1988

Contents

- $54.1 million embezzlement foiled
  - Dave Curry
- Aegis
  - DAve Curry
- Iran Air Incident
  - Bob McKay
- "Binary thinking" misses a lot
  - Bob Estell
- Automatic Air Traffic Control
  - Eldred
- Aviation units of measure
  - Joe Morris
- Mouse trap
  - James H. Coombs
- Threshold probability for declaring a radar blip "hostile"
  - Mike Wellman
  - Clifford Johnson
- Info on RISKS (comp.risks)

$54.1 million embezzlement foiled

Dave Curry <davy@intrepid.ecn.purdue.edu>
Tue, 12 Jul 88 11:22:11 EST

System Crash Fails Swiss Bank Theft (Information Week, July 11, 1988)

Only a chance system crash prevented an attempted computer crime from becoming Britain's, and possibly Europe's, largest recorded theft. A manager at the London branch of the Union Bank of Switzerland issued an instruction to transfer 82 million Swiss francs ($54.1 million) to a branch of Credit Suisse in Lyon, a small town near Lausanne. The payment instruction was sent via the Swift international interbank network, which handles nearly a million payment messages per day.

A computer breakdown at the Swiss end apparently forced the bank staff to

make manual checks of payment instructions that would normally be processed automatically. Suspicions were aroused, and Swiss police were waiting to pounce on the man who arrived to collect the cash. Two men have been arrested in Switzerland, in addition to the London-based, British employee of UBS.

Swift officials in Brussels emphasized that the security of the network had not been compromised, and that what happened was not strictly a computer crime. Genuine computer crimes, in which a secure operating system is breached by an outsider to effect fraudulent transactions, are thought to be rare. [sounds like a rather "convenient" definition to me... -Dave]

More common, and more worrisome to large financial service companies, are cases in which fraudulent transaction instructions received on paper are entered into systems as if they were genuine. The Swift network then has no way of knowing it is carrying a fraudulent transaction.

Protection against these crimes relies on the fact that each transaction is supposed to be ratified by a number of people in different locations. Collusion among several managers would be required for these frauds to succeed. In this case, however, it appears that security at UBS was inadequate: It should not have been possible for one man to enter a fraudulent transaction of such high value [meaning that he should have been able to enter one of lesser value? -Dave] into the Swift network even if it appeared to have come from a genuine telegram ordering payment.

- Philip Hunter, London

--Dave Curry, Purdue University

Aegis

Dave Curry <davy@intrepid.ecn.purdue.edu>
Tue, 12 Jul 88 11:22:11 EST

Aegis System At The Heart Of Vincennes Investigation
(Information Week, July 11, 1988)

Unanswered questions about the Persian Gulf engagement in which the U.S. Navy cruiser Vincennes shot down an Iranian jetliner have focused attention on the Navy's Aegis automated weapon system. Aegis is widely considered one of the most sophisticated uses of automation in the armed forces. Vice Admiral Joseph Metcalf III, Deputy Chief of Naval Operations, has referred to it as "Star Wars at sea."

Part of Aegis' uniqueness is that, like SDI, Aegis is more a concept than a specific weapon system. It was developed by RCA's Missile and Surface Radar unit under a contract to synthesize a weapon system capable of fighting air, surface, and submarine threats simultaneously.

Aegis combines input from four phased-array radars (which employ hundreds of tiny radar beams to scan the entire horizon without causing the gaps in surveillance created by rotating dish radars) - using UYK-7 computers manufactured by Unisys - to create a graphic display of all air, surface, and subsurface targets on video screens in the ship's combat information center (CIC), including information on the target's speeds and direction. The radars scan an area that reaches out in all directions from the ship in

the shape of a bowl or shield, hence the name Aegis.

The ship's sensors also track whether the target is friend or foe, neutral, or assumed friend or foe, based on visual identification or encrypted electronic signals. All of this information - tracks, data, displays - and almost all communications in or out of the ship's CIC is automatically recorded in Aegis' computer.

This is the data Navy investigators will examine when they attempt to discover what went wrong on the Vincennes. Although Secretary of the Navy John Lehman has referred to Aegis as "the most carefully tested combat system ever built," the system was deliberately designed for human input - VISUAL IDENTIFICATION OF TARGETS, OPERATOR ASSIGNED FRIEND-OR-FOE STATUS [emphasis mine], and operator selected targets - and is, thus, subject to human error.

- Christpher Hord

Iran Air Incident

Bob McKay <munnari!cs.adfa.oz.au!rim@uunet.UU.NET>
Tue, 12 Jul 88 13:25:50 EST

Much of the commentary on this incident treats it as 'a land far away in a time long ago'; it's not - it's an immediate question not just for Iran, but the whole of SE Asia and Australasia: ALL the traffic between here and Europe overflies the Gulf, much of it staging through Bahrein or Dubai. Until now that hasn't worried me much - a 747 at 25,000 plus feet ought to be safe, so I thought. But now I wonder - could a DC10 on its final descent into Dubai on an unpredicted track - perhaps avoiding a storm - look like an attack on US vessels? What if an Iranian Mirage had accidentally crossed its track earlier? Even scarier, what if that Mirage deliberately followed it in? Seems like a reasonable way to get closer to the task force vessels. Improbable? So is the present story on mistaking an airbus for an F14. The point is, this was not just an unlucky worst case event; it was actually one of the better possible scenarios from the US point of view - imagine if it had been an Air India or Qantas jet that was downed. The US forces in the Gulf seem to be in a virtually impossible situation. They cannot afford to assume the best - that a target is innocuous until proven otherwise; they also cannot afford to assume the worst - that a target should be blasted unless proven friendly. On the other hand, the airlines involved don't have much alternative either as there are no other corridors available. Further disasters don't seem unlikely from here.

"Binary thinking" misses a lot

"FIDLER::ESTELL" <estell%fidler.decnet@nwc.arpa>
12 Jul 88 08:04:00 PDT

I believe we've previously discussed the "RISKS of 'binary' thinking" in this forum; i.e., recognizing only dichotomies - one/zero, right/wrong ... Our computer thinking - which we sometimes use to debug code - encourages that; ditto our legal system.

In defense of CAPT Will Rogers, I spoke of tragedy; I'd bet that Will agrees with that conclusion. I'd also guess that he would agree with George Will ["This Week with David Brinkley", ABC, Sunday 10 Jul 88] that his actions were "... morally defensible under the circumstances;" BUT that he would not dispute Sam Donaldson's point [ibid.] that the outcome was NOT morally desirable.

Some readers of this journal did not see me blame the USN, so they assumed that I found the "fault" with the Iranians. In fact, I found no fault; if I had, I think I would have suggested we debate the methods [at least, and perhaps motives, too] of those who put USN warships in "harm's way" without bothering to declare war. If others want to pursue that debate, then I suggest we move it to ARMS-D. [arms-d@xx.lcs.mit.edu]

In RISKS, I suggest we have a hard look at the generic problem of doing systems - offensive, defensive, process monitoring, banking ... that ordinarily have, historically, used "binary logic" when indeed they probably ought to evolve into "expert systems" that use NOT ONLY classical logic [e.g., Boolean] BUT ALSO [occasionally] "fuzzy logic." This discussion might quickly spread to include "neural network" kinds of logic, in which the failure of several bits [gates] has only slight impact on the outcome, perhaps not even noticeable.

Bob

Automatic Air Traffic Control

<eldred@apollo>
Mon, 11 Jul 88 20:52:37 EDT

Considering the discussion about the Iranian A300 incident, I wondered about the implications of current efforts to automate air traffic control. Perhaps if the Iranian ATC and the US Navy Aegis system were fully automated then the chances of an unfortunate incident happening might have been different? This article tells of current US plans in that area:

FAA BEGINS PLAN TO FULLY AUTOMATE ATC FUNCTIONS
[from Aviation Week & Space Technology, June 27, 1988, p 73]
[used without permission]

SALT LAKE CITY--FAA Administrator Allan McArtor has begun a three-phase plan to progressively automate air traffic control functions that eventually would automate most functions and limit human controllers to supervisory and emergency functions.

In a speech here dedicating the last of the FAA's 20 Host ATC computer systems, McArtor said the automated network would rely on computers and satellite tracking to choose the best, safest and most fuel- and time-efficient routes for aircraft. It would also space them more efficiently than human controllers can.

The agency already is working on Phase 1 of the automated en route air traffic control system (AERA) plan, McArtor said. When functional, this

computer software upgrade will allow controllers to evaluate routes requested by pilots for potential conflicts with other aircraft, prohibited airspace and flow control restrictions.

The second phase, scheduled to be operational by the late 1990s, would give controllers several solutions to traffic problems. Any route chosen by the controller would be communicated automatically to the aircraft by digital data link.

The final part of the AERA plan--and admittedly the most ambitious, McArtor said--would upgrade air traffic control software to allow totally automatic air traffic operations. Computers would detect and resolve traffic control problems, make decisions, and offer clearances to aircraft without human intervention. However, air traffic still would be supervised by humans, McArtor said....

Satellite tracking and communications technology will be key to the AERA effort and future ATC system modernization, McArtor said

---

Aviation units of measure

Joe Morris (jcmorris@mitre.arpa) <jcmorris@mitre.arpa>
Mon, 11 Jul 88 21:32:15 EDT

Discussing the question of the altimeter display in the Airbus involved in the flyby crash in France in RISKS 7:20, Henry Spencer comments:

<> Does the Airbus model in question display altitude in feet or meters?
> [Question raised regarding whether the Air France Airbus was at 30
> feet or 30 meters...]
>
>Unless I am greatly mistaken, in feet. ...

At the risk of a case of foot-in-mouth disease (since I have no experience flying as a crewmember in Europe), my Jeppesen manuals (flying charts) seem to contradict Henry's comment. The following is extracted from the Jeppesen J-Aid, "Tables and Codes" section, pp. 27-30 (dated 26 February 88):

UNITS OF MEASUREMENTS TO BE USED IN AIR AND GROUND OPERATIONS

So that there would be no misunderstanding as to what units of measure (as mitres or feet) were used in each country, the International Civil Aviation Organization (ICAO) provided a recommended table from which countries could choose either the table labeled "ICAO" or the table labeled "Blue".

In 1979, ICAO revised Annex 5 and replaced the "ICAO or Blue" choice with "International Standard" (SI) and non-SI.
[...]
[excerpts from the definition matrix:]

Measurement of:	ICAO	Blue	SI	non-SI

Distances used in navigation reports	Nautical miles and tenths	Nautical miles and tenths	km	nm
Relatively short distances	metres	metres	m	
Altitudes, elevations and heights	metres	feet	m	ft

[...]
Dimensional units to be used in air/ground communications applicable for the following countries or FIRS: [excerpts]

France: ICAO (8) (60)
Switzerland: SI/non-SI
United Kingdom: Blue (63)
United States: Blue (33)

[Relevant footnotes:]

(8) Altitudes and heights on IAL charts in feet
(33) Relatively short distances in feet [...]
(60) [...]
(63) [...]

There are presently 69 footnotes explaining non-standardized measurements. The international aviation community, in other words, doesn't have the universal system of measurements which would be nice for everybody, and it's not at all unlikely that some pilots could become mixed up over a readout.

On the other hand, anyone who would fly a transport with passengers aboard on a low pass without significant experience at the controls of that make-and-model...

Joe Morris (jcmorris@mitre.arpa)

Mouse trap

"James H. Coombs" <JAZBO%BROWNVM.BITNET@MITVMA.MIT.EDU>
Tue, 12 Jul 88 14:19:49 EDT

A user posted this notice on our bulletin board:

> Subject: Mouse Injury
> Category: Computer hazard
> Text: Add another to the list of computer-induced medical problems. In frantic, last 8 days before publication haste I used the mouse madly in formatting the handbook for employees, and managed to inflame the joint of my index finger so thoroughly that I'm now in a splint and taking nasty pills. Had I known this could cause a problem, I'd have used keyboard commands whenever possible, as I

normally do. [...]

Threshold probability for declaring a radar blip "hostile"

Mike Wellman <MPW@ZERMATT.LCS.MIT.EDU>
Sat, 9 Jul 88 12:05 EDT

Clifford Johnson asks,

> ...at what perceived "odds" -- 50-50, 60-40, 90-10 ? -- does a commander have "sufficient cause" to "declare" a radar blip, that might be hostile or might be a commercial flight, officially "hostile," so as to shoot it down?

The short answer is that there is no such threshold probability. The question presumes the the commander faces a one-shot shoot/no-shoot decision to be taken on the basis of information assessed at an instant in time. More realistically, the commander's options at any instant t are (1) shoot, and (2) wait an increment delta-t and decide again at t + delta-t. During that interval, the ship is either attacked or it gains further information about the blip (the mere absence of an attack counts as information). The "shooting threshold" depends on the time t, the likelihood of attack during the next delta-t, and the prospects for collecting further information in the subsequent time intervals. In the general case, the threshold can behave arbitrarily over time.

If we insist on framing this as a one-shot decision, the commander has two options and there are two basic states of nature distinguished by whether the blip is an F14 or a civilian aircraft. Thus, there are four possible consequences:

C1 - (shoot, F14)
C2 - (shoot, civilian)
C3 - (no shoot, F14)
C4 - (no shoot, civilian)

I suspect that even ranking these consequences by desirability will be controversial, except that C1 and C4 are obviously preferred to C2 and C3. Let du(F14) be the difference in utility between the better and worse actions given the blip is an F14. That is,

du(F14) = u(C1) - u(C3), and similarly let
du(civ) = u(C4) - u(C2).

The one-shot decision recommended by this simple model is to shoot iff the probability that the blip is an F14 is greater than p*, where

p* = du(civ) / [du(civ) + du(F14)].

Note that p* = 1/2 exactly if du(civ) = du(F14), that is if the differences between the "wrong" and "right" actions are the same for both possible states. The threshold is greater or less than 1/2 as the

civilian or F14 consequences are considered relatively more or less significant. It should also be emphasized that these terms are not simply "the value of civilian versus military lives."

Again, this model is outrageously simplistic because it entirely ignores the dynamic nature of the actual decision and the important role of prospective information.

Johnson's second question is

> given the shortness of the response time, what could be the best odds attainable in a realistic attack scenario, even assuming the best computer technology the United States could field?

There are no general limits to the extremity of the posterior odds, regardless of technology, simply because the priors can be arbitrarily extreme. In particular situations, however, limitations of the sensing technology do bound the final assessment.

--Mike Wellman.

Threshold probability for declaring radar blip "hostile"

Clifford Johnson <GA.CJJ@Forsythe.Stanford.EDU>
Sun, 10 Jul 88 13:44:59 PDT

> ...at what perceived "odds" -- 50-50, 60-40, 90-10 ? -- does a
> The short answer is that there is no such threshold probability...

Yes and no, mostly no. Time passes, and in all circumstances what you say holds true only until a "use them or don't use them" decision deadline dictated by the particular threat perceived. After this time, the intended defense is ineffective. Curiously, in the Iran shootdown it has been reported that the decision came a little late, which perhaps suggests that the Captain panicked just when the flight turned towards its center corridoor, which happened to be in the direction of the ship. This would mean that the flight was shot down *because it responded* to the strident warnings. If the threat of missile attack had been usual (supposing arguendo that F-14's could deliver missiles), the plane would have been hit after it had released its missiles.

I don't contest your game theory -- such utilities are increasingly being incorporated into online military battle managers. In the envisaged naval battle management system, the decision would presumably be recommended in such utilitarian terms to the Captain or remote Admiral. This means that such values as we have speculated about really are being written into military hardware that actually or virtually executes its own Rules of Engagement. I shudder.

> given the shortness of the response time, what could be the best
> odds attainable in a realistic attack scenario, ...
> There are no general limits to the extremity of the posterior odds, ...
> In particular situations, however, limitations of the sensing technology

> do bound the final assessment.

The final point counts, I agree, but an uncontrolled risk-amplification may in general occur in real-time guestimation of the background or a priori probabilities of a threat. Calling an alert, or issuance of a strategic warning, which is what the Gulf forces got over the July weekend, does exactly that, it vastly distorts a priori probabilities. And I say "distort" with academic rigor, for it is a well-proven tenet of war that a strategic warning is highly unreliable but easy to believe. Just like a sale isn't final until a check is signed, or rather, until the computers say so, so hostilities may not occur until a first shot is fired, or rather, until the computers say so. Then the firing of the first shot then places a priori odds beyond reason, permitting a commander to see threats even from directions that shots have not been fired from.

Clearly, it is in everyone's interests that a priori probabilities of conflict are not unreasonably figured. Without questioning good military intentions, I am concerned that the likelihood of civilian deaths features insufficiently in the U.S. Rules of Engagement. Witness the destruction of a mental hospital in Grenada, of many civilians in the Libyan raid, and now of a civilian jet -- and so far, the military has not been faulted for any of these mishaps, on the basic grounds that civilian deaths were due to tragic technical glitches tolerable in the circumstances.

I am most concerned that the nuclear SIOP implicitly contains a priori estimates of threat probabilities which are unreasonably boosted to protect the Air Force and the defense establishment. This in effect devalues civilian consequences, and heigthens the danger. And yet the nuclear hair-trigger is so unopposed that the Strategic Air Command is *celebrating* 1988 as "The Year of the SAC Alert Force," in commemoration of the 30-year-old alert called for SAC's bombers on October 1, 1957.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 22

Thursday 14 July 1988

Contents

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

A-320 Airbus Crash Inquiry

Brian Randell <Brian_Randell%newcastle.ac.uk@NSS.Cs.Ucl.AC.UK>
Tue, 12 Jul 88 21:31:25 +0100

Today's Guardian carried a story with a new and alarming slant. It is reprinted here in toto, without permission.

AIRBUS INQUIRY OBSTACLES FUEL COVER-UP FEARS

[By] Paul Webster in Paris

An attempt to stop an examining magistrate investigating the cause of the A-320 airbus crash in eastern France last month has raised doubts over official claims made immediately after the crash that pilot error was the only cause.

Mr Germain Sengelin, the senior examining magistrate at Mulhouse, defied a Justice Ministry order yesterday to drop a judicial inquiry and said that he could understand that there was official concern that "the search for truth was being placed above other interests."

The magistrate was told to hand over the inquiry to a judge but continued questioning witnesses. He was concerned that the Airbus's two flight recorders were taken away after the crash by Transport Ministry officials. He said the recorders had not been sealed to "guarantee their authenticity and integrity."

He was also angry that the local public prosecutor, who is responsible to the Justice Ministry, had already decided that pilot error was the cause of the crash which killed three passengers during an aero-club joyride flight. More than 130 other people escaped when the low-flying Air France chartered jet crashed into a wood.

Air crew trade unions have also stepped up their protest over the plane's dependence on a revolutionary computer fly-by-wire system operated by a two-man crew. The air crews, who believe a flight engineer is needed to oversee the ultra-modern equipment which is supposed to correct pilot error, said there was a moral question involved. The policy of a two-man flight crew was putting passenger lives in danger. Pilots on France's domestic airline, Air Inter, began a new strike last night as part of a three-year campaign over Airbus safety.

With the judicial and Transport Ministry inquiries, there are three investigations being made into the accident, the third being by Air France.

But before any investigating team was able to give a point of view, the flight recorders had been analysed by civil aviation officials and the main finding revealed by the Transport Minister at the time, Mr Louis Mermaz.

He ruled out any possible fault in the plane's design and blamed the pilot. As the Airbus is Europe's main challenger to US civil aviation supremacy, Mr Mermaz was concerned that doubts over the computer system could affect orders from more than 50 airline companies for about 500 A-320s which sell for about (pounds)20 million.

User interface problem in the Aegis system?

Kee Hinckley <nazgul@apollo.com>
Wed, 13 Jul 88 10:47:46 EDT

Something mentioned briefly in newsweek's analysis of what happened is that the display system does not show the actual radar blip, but rather an icon which indicates information about the object (under/on/above water and friendly/unknown/ enemy). Although at the 20 mile range there would be no difference in blip size, they asserted that a dumber radar system might have seen a difference at the distance at which missles were fired. If this is true it is a good example of an instance where switching to a symbolic display resulted in a loss of potentially critical information.

(Of course the blip size is still not a good indication of aircraft type, given reflectivity differences, but any bit of information can help.)

Kee Hinckley, User Environment, Apollo Computer Inc.

Radar cross sections, Flt. 655, and F-14s

Eugene Miya <eugene@amelia.nas.nasa.gov>
Thu, 7 Jul 88 20:06:23 PDT

Please do not mistake the visual cross-section of a target to equal a radar cross-section. Radar is a less than exact science, all cross-sections are determined empirically with a anechoic chamber.

A good example to understand this is the B-52, which comes with a drone called a Quail. The Quail is a tiny fraction of the B-52's size but is designed to give an identical signature (not quite). Several radar references include a recent Spectrum article on radar cross-sections (the IEEE will now probably do A320 and 655 article as they did they award winning Stark article). There is also Skolnick's book on radar.

Current thinking is also based on active transponders, not on cross-section.

--eugene miya, NASA Ames

GM Blames Computer for Smelly Vans

Peter G. Neumann <NEUMANN@csl.sri.com>
Thu 14 Jul 88 11:29:44-PDT

(UPI) Detroit
Owners of some General Motors vans have been advised not to blame a rotten-egg smell on their companions but rather on the vehicles' computer.
GM has discovered that under certain conditions, 1987 Chevrolet Astro and GMC Safari vans with 4.3 liter engines and overdrive transmissions spew an exhaust with the unmistakable smell of rotten eggs.
The company has issued a bulletin to dealers with instructions on how to fix the problem. Among the remedies is replacement of the computer, which monitors the engine's fuels mix.
The computer in question is used only in vans with overdrive transmission, the Detroit News was told by a GM service technician. An improper fuel mix

results in the buildup of a sulfur and hydrogen mixture, causing the odor, the technician said. [San Francisco Chronicle, 14 July 1988, p. A11]

Lockpicking at Los Alamos

Gary McClelland <MCCLELLAND_G%CUBLDR@VAXF.COLORADO.EDU>
Tue, 12 Jul 88 09:08 MDT

Anyone interested in the recent discussion of lockpicking and security would enjoy reading Richard Feynman's hilarious chapter on his lockpicking adventures at Los Alamos during the bomb building days. The chapter is in his collection of autobiographical stories entitled "Surely You Must be Joking, Mr. Feynman. Reproducing excerpts here would spoil the fun. If the locks to the atomic secrets were so easy to pick it is hard to imagine what system would be required to guarantee no burglars get in the house. Just keep the insurance premiums paid and make it look like your house would be a bit more troublesome than the neighbor's.

Gary McClelland (Univ of Colorado)

supposedly-unique id. no. from non-unique personal characteristics

Larry Margolis <MARGOLI@ibm.com>
12 Jul 88 12:31:37 EDT

New York State also encodes the driver's sex and date of birth in the driver's license number. The reason for this is that a police officer can do a quick check to tell if the license is invalid. (No guarantee that it's valid, of course, but if the DOB on the license doesn't match the encoded version, or the sex isn't encoded properly, you know that it's invalid.)

Larry Margolis

NJ Driver's license number coding

<SROBBINS%DREW.BITNET@CUNYVM.CUNY.EDU>
Mon, 11 Jul 88 16:41 EDT

tab@mhuxu.att.com writes:
> I had to laugh at "The Eyes Have It". The last five digits of my NJ
>driver's license number are 61664. This is supposed to represent my
>date of birth and eye color. I was born on 11-22-66, and the last time
>I checked my calendar, we didn't even have 61 months!

On NJ driver licenses, the first 4 of the last 5 digits are always the month and date you were born. If you were born in October, November, or December, the first '1' is replaced by a '6' , hence 6166 for those four digits on your license. I *think* this is always the case for people born in those three months; other numbers might be used in place of the '1'. My mother was born in October, and the numbers on her license are 60422 for the last

five digits. The last number on your license is your eye color; if you have a picture license, the codes for numbers and eye colors are on the back of the license card. You might also note that of the second group of 5 digits, the first two should be '66' in your case, because you were born in 1966. The reason for doing all of this is because NJ picture driver's licenses are very easy to alter for ID purposes (to buy alcohol, etc.) - so the DMV figured they'd get smart and build the birthdate into the DL number. Except now everyone knows the secret and it's pretty useless. I believe all the numbers on a license mean something --> another thing they try to protect against is people replacing the picture with another (also very easy on a NJ picture license).

Scott Robbins SROBBINS@DREW.BITNET

Colwich Junction, England, 1986

Mark Brader <msb@sq.com>
Wed, 13 Jul 88 18:20:35 EDT

The official report on a train collision* at Colwich Junction, England, on September 19, 1986, has been released and is written up in the June issue of Modern Railways magazine. There are two RISKS-related points.

*Both trains had electric lomocotives, which collided. The northbound train was supposed to stop; the southbound one was running at 95 to 100 mph. Of "nearly 900" passengers on the two trains, 75 were injured, 32 requiring hospitalization, but the only fatality was the southbound train's driver.

The basic cause was driver error. The error related to "approach-controlled" signals, where a restrictive aspect is used merely to force the train to slow down, rather than its original meaning of "prepare to stop". In some cases new flashing aspects are used to indicate approach control, but the exact meaning varies (it would take too long for me to go into detail here). The driver assumed that a particular red signal was going to clear as he approached, when it was actually telling him to stop, hence the accident.

The magazine editorially blasted the present inconsistent system, saying that approach control, which is supposed to stop trains from taking junctions too fast, "is now a lethal menace because it does different things in different places and is bound to lead drivers into confusion". They call for a system with the desired speed explicitly displayed.

There was a further contributing cause. The northbound train was equipped with wheelslip protection, i.e., antilock braking, which a witness heard in operation. (Why do trains need antilock braking when they don't have to steer? Because if the wheels slide, flat spots are worn onto them, causing bad riding and premature wear.)

The driver had no way to turn the wheelslip protection off. If he had had, the accident might have been avoided; experiments to test this were inconclusive, it being too difficult to reproduce the exact conditions.

But an override would certainly have reduced the stopping distance, and the report recommended that wheelslip protection be automatically turned off when the driver selects emergency braking.

Mark Brader "What can be more palpably absurd than the prospect held out
utzoo!sq!msb of locomotives travelling twice as fast as stagecoaches?"
msb@sq.com -- The Quarterly Review (England), March 1825

Shades of Fantasy in Real-Life -- group games

<mcvax!doc.ic.ac.uk!acwf@uunet.UU.NET>
Thu, 14 Jul 88 14:23:36 BST

I noticed the following article in UK Micro Mart magazine and thought it might indicate some hitherto unforeseen risks of computer use!

Melanie Weaver and Jez Thorpe, both avid users of Telemap Groups Shades game, have become the first couple to marry after meeting in a multi-user computer game. The newly-weds met in Shades, where players exist in a fantasy world of castles, wizards and buried treasure. Their characters married in the game; then they were engaged for real a month later, and married recently at a church in Cornwall. Melanie, who works in the travel business said: ``When I started playing the last thing on my mind was that I would meet my future husband through a computer game. But I soon discovered that one of the best things about Shades is that it allows you to meet lots of interesting people.''

Shades is a multi-user adventure set in a fantasy world where players attempt to rise from the rank of novice to wizard by collecting treasure and scoring as many points as they can. With up to 128 players taking part the characters you encounter -maybe in the on line pub, The Talking Shoppe - could be using a computer anywhere in the world.

IQ measurement by machine?

Mark Brader <msb@sq.com>
Thu, 14 Jul 88 13:42:42 EDT

The following article by Bob Gray of Edinburgh University appeared in sci.misc as an outgrowth of an exchange about the high-IQ society Mensa.

The risks associated with these machines would seem to be of the same type as those associated with the use of polygraph machines as if they were lie detectors.

Mark Brader, SoftQuad Inc., Toronto

(Forwarded text follows. The quoted paragraph is from an earlier article by Chris Long in the same newsgroup.)

> Binet originally designed his tests to detect mental deficiency, which
> they do, up to a point. Alas, things did not stay there. Goddard,

> Terman, and Thorndike took things to where they are now.

Just to add some more napalm to the postings...

A company in Guildford, Surrey, UK announced last week that they are to market a device to directly measure the early signs of diseases affecting the brain. Alzheimer's disease and senile dementia were mentioned.

Electrodes are attached to the scalp and the electrical activity of the brain in response to computer controlled stimulus is measured.

The device is also claimed to be able to measure IQ.

The report then went on to mention that some companies have already expressed an interest in the device for selecting people with low intelligence to do boring and repetitive jobs.

This device may be an application of some research here at the University of Edinburgh which showed a correlation of greater than 0.6 between scores on IQ tests and direct EEG measuremernts of the speed at which the sensory areas of the brain can process information.

Bob

Aviation units

<Richard.S.D'Ippolito@sei.cmu.edu>
Thursday, 14 July 1988 11:17:32 EDT

It's curious how errors creep in everywhere. In Joe Morris's discussion of aviation units, he reproduces a segment of a table from Jeppesen showing SI units of distance as "km", where the correct unit is "Km". Would an SI person also interpret the non-SI column entry "nm" as "nanometers" and reject the chart?

A manual purporting to set a "official standard" for safety purposes, assuming that the error wasn't a copy error, has an incorrect symbol used for a unit modifier -- kilo is ALWAYS uppercase as are all SI prefixes that multiply as opposed to those representing fractional parts, which are lowercase. (E.g., m = milli = 10^-3 and M = mega = 10^6.) "kg" is NOT an SI unit, but Kg is! Imagine drugs if mg could be milligrams, micrograms, or megagrams, or radiation if mCu were hastily written for microcuries. Some of the folks in my particular field, the electronic, still mark capacitors with mF for microfarads and mmF for micro-microfarads when they should be uF (greek letter micro) and pF (pico = 10^-12).

Yes, we in our leisure know what is meant, but why should the burden be on the reader to interpret, especially in a critical situation? And why the mixed units? All units in a table should be consistent, defined, or spelled out, so that nm, n.m., na. mi., are OBVIOUSLY nautical miles, and not nanometers. To have adjacent lines of a table showing kg and nm (mixed

units with one incorrectly spelled) is irresponsible and, well, risky.

And all those footnotes? They tell me that there is no standard.

RISKS and PGN Saturation!

Peter G. Neumann <Neumann@KL.SRI.COM>
Wed, 13 Jul 88 17:54:20 PDT

The RISKS backlog is up to 50 unfielded messages just in the past week. Many of the pending messages are marginal, and will probably not surface. Many are purely speculative, and those have to be very carefully written in order to be worthy. Others are interesting, but drifting further and further afield -- as seems to happen whenever a subject develops. Others continue to dwell on topics that have already been covered. I realize some of you are receiving RISKS only after long delays (days, in some cases even weeks), which makes it very hard for you not to avoid duplication of messages that you have not even seen yet! But bear with me as I continue to wrestle with the balance between an open forum and a manageably readable, interesting forum. Thanks. Peter

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 23

Saturday 16 July 1988

Contents

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

Policy Chief Indicted in Computer Misuse

owen blevins <blevinso@silver.bacs.indiana.edu>
Fri, 15 Jul 88 20:25:50 est

From New York Times Friday., July 15, 1988:

Metro-North Police Chief Indicted in Computer Misuse

The police chief of the Metro-North Commuter Railroad was indicted yesterday on charges that he improperly used a New York State polic computer system to investigate job applicants, their relatives and people who were suing the railroad.

The indictment against the chief, John V. Esposito, includes allegations of

"computer trespass." Authorities said he is believed to be the first police official to be prosecuted under a 1986 law restricting the use of confidential criminal justice records compiled in computers.

After pleading not guilty in a courtroom in Manhattan, Mr. Esposito, who was released without bail, said his use of the computer system "is standard operating procedure" by police chiefs throughout the state as part of routine background examinations of prospective employees.

Data for Iran airliner discussion

Dave Fiske <davef@brspyr1.brs.com>
14 Jul 88 21:28:21 GMT

I know this is the net, but I hope I can be forgiven for doing a bit of actual research! Here are a few excerpts from some books I happen to have at home. Shows that with just a little effort, we could be having discussions based loosely on fact, rather than vague memories and opinions.

First of all, despite Reagan's statement, the AEGIS system is a bit more than your average radar unit. The following excerpt indicates that it does some interpretation of the data it obtains, and even performs limited decision-making.

> "The AEGIS Combat System was developed to counter the saturation missile attacks which could be expected to form the basis of Soviet anti-carrier tactics during the 1980s. Conventional rotating radars are limited both in data rate and in number of target tracks they can handle, whereas saturation missile attacks require sensors which can react immediately and have a virtually unlimited tracking capacity. The solution adopted in the AEGIS system is to mount four fixed planar antennae each covering a sector of 45 degrees on the superstructures of the ship. Each SPY-1 array has more than 4000 radiating elements that shape and direct multiple beams. Targets satisfying predetermined criteria are evaluated, arranged in sequence of threat and engaged, either automatically or with manual override, by a variety of defensive systems."
>
> John Jordan, "An Illustrated Guide to the Modern U.S. Navy", 1986, Prentice Hall.

Several people have maintained in comp.risks that the F-14 would not be much of a threat to surface ships. However:

> "The twin-jet F-14 is indeed some airplane. It was designed to range farther, fly faster, climb higher and pack more wallop than any interceptor ever built. While it possesses some of the features of a fighter, fighter pilots certainly would prefer to call it an interceptor. Its long suit is its fire control system and its missiles. With his AWG-9 radar and infrared-sensor-computer system, the backseat Missile Control Officer (MCO) of the Tomcat can track twenty-four separate targets, from sea level to one hundred thousand feet, up to one hundred miles distant."

James W. Canan, "The Superwarriors", 1975, Weybright and Talley.

"Possibly the most complete fighter in the world today, the Grumman F-14 Tomcat first entered service in 1975. Armament consists of M61A1 20-mm rotary cannon plus AIM-9 Sidewinder short-range, AIM-7 Sparrow medium-range and AIM-54 Phoenix long-range air-to-air missiles. A combination of all these missiles can be carried at one time, making the F-14 capable of shooting down any flying intruder at any range up to 200 km (125 miles). The Phoenix missiles are operated in conjunction with the Tomcat's AWG-9 radar, and can hit targets at any altitude from ground level to over 2400 m (78,740 ft)."

"Modern Combat Aircraft", Crescent Books

According to The Military Balance, 1984-85, published by the International Institute for Strategic Studies, Iran still has 10 F-14As (in 1975 they had 15--some undoubtedly have become inoperative since then), and does have Sidewinders, Sparrows, and Phoenixes.

Dave Fiske (davef@brspyr1.BRS.COM)

Re: Data "viruses" (RISKS-7.11)

Peter J. Denning <pjd@riacs.edu>
Fri, 15 Jul 88 14:47:45 pdt

Dave Horstall inquired about whether the propagation of corrupted data through a system can be considered a new form of virus. No.

The propagation of corrupted data is an old problem that systems designers interested in fault tolerance must face. It is a difficult problem and many systems do not include appropriate data consistency checks to prevent or mitigate it.

The virus is a program designed to infect other programs with copies of itself and to perform unwanted actions in the manner of a Trojan horse.

Peter Denning

Program viruses vs "data viruses"

Peter G. Neumann <Neumann@KL.SRI.COM>
Sat, 16 Jul 88 10:29:19 PDT

On viruses versus data propagated effects of contaminated data:

Yes, the propagation of corrupted data is an old problem, although it is generally considered within the scope of a single program or a single process. My favorite example of more global propagation is provided by the ARPANET collapse (mentioned in RISKS occasionally, but newer readers should dig up Eric Rosen's enlightening article, "Vulnerabilities of network control protocols",

in ACM Software Engineering Notes, vol 6 no 1, January 1981). This was caused by a status word being propagated along with two corrupted versions of itself -- as a result of hardware malfunctions. The consequence was that those two corrupted versions (yes, propagated by the normal node programs, which were unaltered) contaminated every node in the network -- because the flawed garbage collection algorithm broke down. True, there was no program virus. However, the two bogus status words effectively contaminated the entire network! This case is interesting not because a piece of data was altered, but because three different versions of the SAME piece of data were able to bring the entire network to its knees -- despite the belief that distributed control was safe. That kind of contamination deserves some sort of explicit identity such as "data bacterium" or "data microbe" or whatever, although it has some of the characteristics of a (data or nonprogram) virus... PGN

Invitation to visit Disaster Research Center (DRC)

Disaster Research Center <ACJ00984%UDACSVM.BITNET@CUNYVM.CUNY.EDU>
Fri, 15 Jul 88 20:24:21 EDT

An Introduction to the Disaster Research Center for RISKS Readers. Come to our open house in August !

The Disaster Research Center, the first of its kind and the only one in the United States, was established at the Ohio State University in 1963 and moved to the University of Delaware in 1985. The Center engages in a variety of sociological and social science research on group and organizational preparations for, responses to, and recovery from community-wide emergencies, particularly natural and technological disasters. Since the Center's inception, there have been over 496 different field studies. Teams have gone to earthquakes in Japan, Chile, Yugoslavia, Italy, Iran, El Salvador, Greece, California, and Alaska; hurricanes in the southern and eastern United States, as well as Japan; floods in Italy, Canada, and more than a dozen states; and tornadoes and hazardous chemical incidents in Canada, Mexico, and the United States. A dozen cities struck by major disasters have been restudied several years after the initial research. For purposes of comparison, Center personnel have also examined organizational responses to civil disturbances and riots.

The Center has a number of professionals on its staff plus supporting clerical and secretarial personnel. It is directed by Professor E.L. Quarantelli, with the assistance of Professors Dennis E. Wenger and Russell R. Dynes, all of the Department of Sociology at the University.

Recent studies have focused on: Social and organizational aspects of the delivery of mental health services and of emergency medical services in mass emergencies; and socio-behavioral responses to acute chemical hazards and the problems involved in mass evacuation and sheltering. Research underway includes the ways in which information relating to disaster is processed through news organizations, the organizational and public response to the Mexico City earthquake, and the role of local emergency response agencies. Center personnel have examined legal aspects of governmental responses in disasters, the emergence and operation of rumor control centers, mass media reporting of community crises, the functioning of relief and welfare groups in

stress situations, and the handling of the dead in catastrophes.

The research provides basic knowledge about group behavior and social life in large scale community crises as well as information which can be applied to develop more effective plans for future disasters. Besides storing its own data collected through in-depth interviewing, participant observations, and document gathering, the Center serves as a repository for materials collected by other agencies and researchers. The Center's specialized library, which contains the world's most complete collection --over 20,000 items-- on the social and behavioral aspects of disasters, is open to all interested scholars and public and private agencies involved in emergency planning. With over 400 publications, the Center has its own book, monograph, and report series. There are close relations with Canadian, Mexican, Australian, Swedish, Japanese, and West German disaster researchers, a number of whom have been visiting research associates at the Center for periods of up to a year, and collaborative field research is currently underway with groups in Japan and Mexico. An exchange program and very close ties with Italian researchers, especially the Mass Emergency Program of the Institute of International Sociology in Gorizia, Italy.

Center activities have been supported by diverse sources including the Health Resources Administration; the Center for Applied Social Problems, National Institute of Mental Health; the Defense Civil Preparedness Agency; the Water Resource Research Program, Department of the Interior; the State of Ohio Department of Mental Health; but major funding has been from the National Science Foundation, and the Federal Emergency Management Agency.

If you would like more information concerning the Disaster Research Center or desire an updated Publications List, write to Margie Simmons, Office Coordinator, Disaster Research Center, University of Delaware, Newark, Delaware, 19716, United States of America.

** Special note to Risks Digest Readers **

Anniversary Celebration Announcement

The Disaster Research Center was formed in August, 1963.
Thus, it will be 25 years old next month.

To mark the occasion, an open house will be held at the Center's present location on the third floor of 102 East Main St., Newark, Delaware (U.S.A.).

Time: Monday, August 22, 1988
1 - 5 p.m.

We hope you can take some time to visit us.

- E.L. Quarantelli, Director
- Russell R. Dynes
- Dennis E. Wenger

(Information forwarded by Bruce D. Crawford, Computer Services Coordinator, Disaster Research Center).

Passwords on networked systems

Steve Oualline <horizon!sdo@seismo.CSS.GOV>
15 Jul 88 22:31:51 GMT

Although RISKs seems to be primarily oriented toward major problems with the cutting edge of technology, I wish to offer an example of a small problem that can be solved by a little common sense.

At our site we have several UNIX systems running on a network. For convenience of the administrator, me, all the root passwords are the same. I discovered the hard way that this is not a good idea. I wanted to reboot "zabbar" a small system that no one was using, so I walked over to its console and type su root, /etc/halt.

This shut down the system -- the problem was that I had done rlogin horizon (horizon is our main system), and had shut it down by mistake. If the root passwords had been different for each machine, then horizon would have rejected the root password for zabbar causing me to discover which system I was really on.

Other ways to manage risks (Re: RISKS-7.20)

Dave Fiske <davef@brspyr1.brs.com>
15 Jul 88 18:58:58 GMT

> From: Doug Faunt (phone (415) 496-4727) <faunt@spar.slb.com>
> Subject: re: lockpicking and burglars
> I would like to point out that it might be worthwhile to improve your
> locks to some degree, ...
> ... You may not be able to keep them out, but you can make sure there's a
> record.

I'm surprised that comp.risks readers are primarily fixating only on PREVENTION for managing risks. Prevention is only one way to deal with them.

Nearly all homeowners therefore have insurance to cover the theft of contents, as well as locks on the doors. Some have burglar alarms as well. The prevalence of insurance and burglar alarms is an indication that unwanted entries cannot be 100% eradicated. Locks are only one aspect in the management of the risk of theft.

The existence of law enforcement agencies is another deterrent--a burglar has to (well, at least he should) consider the possibility that he will get caught. The consequences of entering a locked home ("burglary", or "breaking and entering") are more severe than entering one which is not locked ("illegal entry"), and is also more easily proved due to physical evidence.

In addition to helping to deter entry, locks help to provide evidence

to facilitate getting an insurance settlement, or to capture the culprit and achieve return of the goods.

Similarly, a computer system can probably never be made totally secure, since it's always possible (granted, very unlikely) that an unauthorized user could happen to guess a correct password on the very first try, etc. However, log files are kept and checked, means of disciplining system abusers are maintained, backup tapes are made, etc. as further means of reducing the consequences of tampering.

Dave Fiske (davef@brspyr1.BRS.COM)

[But don't forget that in many systems it is easy to turn off auditing altogether, or to bypass it, or to modify the audit trail later. PGN]

Colwich Junction, England, 1986 (Re: Mark Brader, RISKS-7.22)

Blair P. Houghton <bph%buengc.bu.edu@bu-it.BU.EDU>
Fri, 15 Jul 88 17:50:38 edt

Mark's message points out a common misconception: that skidding provides more stopping force than does rolling with the brakes on.

The truth is that the coefficient of friction is lowered drastically once the surfaces involved begin to slide. That is, the kinetic coefficient of friction is lower than the static coefficient of friction.

Hence, a rolling wheel, which indeed has a nonsliding portion of its surface in contact with the rail, can apply more force to the rail, thus slowing the train faster; once the wheel locks up and begins to slide, the force decreases in a virtual discontinuity, and the train slows slower, meaning that the stopping distance is larger (usually much larger).

If the wheelslip protection overcompensated for impending slippage by lowering the braking force below even the skidding-friction force, then it is utterly at fault for an extended stopping distance, and the above mentioned report's conclusion is correct.

However, if the wheelslip protection was properly designed, it should have operated in the region between skidding-friction force (kinetic coefficient in effect) and onset-of-skidding force (static coefficient in effect), then the report is dangerously wrong and has made a suggestion that will aggravate future accident situations.

While the "flattening" argument for wheelslip protection is good economy, the increased stopping power is the primary reason that antilock braking was invented, since saving lives is the best economy.

Blair P. Houghton

Oops -- risks of writing -- SI prefixes

<Richard.S.D'Ippolito@sei.cmu.edu>
Friday, 15 July 1988 09:29:09 EDT

I blew it. The SI prefixes for kilo (10^3), hecto (10^2), and deca (10^1) are abbreviated with lower case letters. Those above kilo are abbreviated with capital letters. All those below (10^-1 to 10^-18) are lowercase. I've seen too many KVs and KWs in the electrical industry. I'm sorry -- next time I'll look it up first.

Rich

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 24

Monday 18 July 1988

Contents

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

The IRS Illinois Experiment

<sun!portal!cup.portal.com!Patrick_A_Townson@unix.SRI.COM>
Sun Jul 17 14:01:44 1988

The Internal Revenue Service says it wants to make it faster and easier for taxpayers to get their refunds in the future, so it is experimenting with a new approach in Illinois during the 1989 tax paying season.

As a resident of Illinois, you will be able to file your tax return electronically, by hooking into the IRS computer to complete your tax return and provide the necessary information on your income, taxes withheld, etc.

The IRS says if this experiment goes as planned, it will speed processing of tax returns by fifty percent, allowing refunds to be paid within three weeks instead of the usual five or six weeks. As to be expected, it is not all altruism on the part of the Internal Revenue Service.

A return sent to the IRS electronically costs about $9 to process. A paper return mailed to the agency costs $72.50. The reduced labor costs will save the revenuers about $200 million over the next ten years, primarily through reduced labor costs, filing space and paper work.

The agency will still have some paper mail to process, since even the returns filed electronically will require a signature form to be mailed in along with W-2 forms, but the work will be cut down drastically from the current system.

The IRS believes the lure of a faster refund, which can be deposited directly into a financial institution, will motivate taxpayers to file earlier. If their theory is correct, and if the "Illinois Experiment" works out as planned, the electronic filing program will be expanded nationwide over the next 2-3 years.

Taking advantage of the electronic option will cost taxpayers in other ways, however. The computer link will only be available through tax preparation services. The IRS believes that offering access to their computers to all personal computer users would cause them 'some concerns about hackers and phreakers getting after us, making trouble for us..', coordinator of the new program in the Chicago IRS offices, Regina Nixon said.

She said the agency is looking at ways to allow personal computer users to plug directly into the system while at the same time keeping the system secure, but nothing has been decided yet. She said one possibility will be that terminals will be provided in IRS offices where the public can come in, sit down and work, under the 'guidance' (watchful eye, perhaps?) of IRS employees.

Linda Jordan, of H&R Block, the national tax preparation service based in Kansas City said they will probably charge an additional fee of $18-30 per electronic filing to cover their own costs for the program. She noted that the popularity of the program at first would depend in large part on the amount of the refund and how quickly the taxpayer was interested in getting it.

The new electronic filing program will only be for people with refunds coming. Those folks who owe money will still have to pay the old-fashioned way, by writing a check which is enclosed with a paper return. Taxpayers in Illinois can begin using this new option later this year as they begin the process of reporting their 1988 income. The new electronic system is expected to receive its biggest workout during the first quarter of 1989, and the results of that test will detirmine to what extent it should be promoted nationally.

Dixon, of the IRS office, said they had not yet figured out a way to induce people to file early when they had to pay additional money; but one thing under consideration is to combine the electronic filing approach with a slight discount to the taxpayer who authorizes an automatic draft from their bank account to pay the taxes due.

Now dear Risks Readers: Can't you *just see* and *just imagine* the several possibilities for corruption here on the part of the tax preparation services and others? The theory that it will be more efficient sounds great, but oh what havoc it will cause if the 'wrong people' start diddling the computers!!

Aegis testing data withheld from Congress

Gary Chapman <chapman@csli.stanford.edu>
Mon, 18 Jul 88 09:35:15 PDT

Defense Week reports that an unclassified report of the General Accounting Office (GAO) reveals that the Navy withheld testing problems of the Aegis air defense system from the Congress. "Personnel and Aegis equipment were not subjected to targets or tactics that would be found in combat," and the reports sent to the Congress by the Navy omitted "unfavorable test results." The GAO said that the favorable assessment of the Aegis system by John Krings, the head of testing for the Pentagon, "was not supported by the evidence." The Navy report to the Congress, says the GAO, "potentially led Congress to fund weapons systems whose true operational effectiveness and suitability are unknown."

Gary Chapman, Executive Director,
Computer Professionals for Social Responsibility

"Man in the loop"

Rodney Hoffman <Hoffman.es@Xerox.COM>
18 Jul 88 09:08:10 PDT (Monday)

The July 18 Los Angeles Times carries an op-ed piece by Peter D. Zimmerman, a physicist who is a senior associate at the Carnegie Endowment for International Peace and director of its Project on SDI Technology and Policy:

> MAN IN LOOP CAN ONLY BE AS FLAWLESS AS COMPUTERS.
>
> [In the Iranian Airbus shootdown,] the computers aboard ship use artificial intelligence programs to unscramble the torrent of information pouring from the phased array radars. These computers decided that the incoming Airbus was most probably a hostile aircraft, told the skipper, and he ordered his defenses to blast the bogey (target) out of the sky. The machine did what it was supposed to, given the programs in its memory. The captain simply accepted the machine's judgment, and acted on it....
>
> Despite the fact that the Aegis system has been exhaustively tested at the RCA lab in New Jersey and has been at sea for years, it still failed to make the right decision the first time an occasion to fire a live round arose. The consequences of a similar failure in a "Star Wars" situation could lead to the destruction of much of the civilized world. [Descriptions of reasonable scenarios ....]
>
> The advocates of strategic defense can argue, perhaps plausibly, that we have now learned our lesson. The computers must be more sophisticated, they will say. More simulations must be run and more cases studied so that the artificial intelligence guidelines are more precise.
>
> But the real lesson from the tragedy in the Persian Gulf is that

computers, no matter how smart, are fallible. Sensors, no matter how good, will often transmit conflicting information. The danger is not that we will fail to prepare the machines to cope with expected situations. It is the absolute certainty that crucial events will be ones we have not anticipated.

Congress thought we could prevent a strategic tragedy by insisting that all architectures for strategic defense have the man in the loop. We now know the bitter truth that the man will be captive to the computer, unable to exercise independent judgment because he will have no independent information, he will have to rely upon the recommendations of his computer adviser. It is another reason why strategic defense systems will increase instability, pushing the world closer to holocaust -- not further away.

Aegis

Charles Daffinger <cdaf@iuvax.cs.indiana.edu>
Sat, 16 Jul 88 17:08:02 EST

For a good overview of AEGIS, you may wish to check out:

Adam, John A. _Pinning Defense Hopes on Aegis_, IEEE Spectrum, 25:6, pp 24-27, June 1988.

-charles

Lightning strikes... (again?)

Don Mac Phee <NKK101%URIMVS.BITNET@MITVMA.MIT.EDU>
Mon, 18 Jul 88 09:51 EDT

I recently discovered the RISKS of an insufficiently grounded building the hard way. Lightning struck!

For several years the VAX systems that have existed in this hall at the University of Rhode Island, have been plagued with an unusual number of system crashes. All of these crashes coincided with electrical storms. Unfortunately, no one bothered to research the problem, until now. A simple system could have saved up to thousands of dollars in equipment.

The campus sprawls down the side of one of the higher hills in the area. The building is a four story building, which resides at the top of the hill. The VAX resides on the third floor of this four story building. But there are no lightning rods on the top of this building to dissipate the force of a lightning strike! So the VAX has acted as the perfect lightning rod, generating a positive electrical field sufficient enough to attract lightning.

Thousands of dollars have gone to solve a problem that a four dollar

rod, and 20 dollars worth of wire could have solved.

Don Mac Phee

p.s. All standard and some non-standard disclaimers apply. I do not represent the University. I just comment on it.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 25

Wednesday 20 July 1988

Contents

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

Possible reason for unexpected Audi 100 acceleration

LARS LINDWALL LIDAC <<L_LINDWA%SELIUC51.BITNET@CUNYVM.CUNY.EDU<>
Tue, 19 Jul 88 18:00 N

The following is what I can recall from a news story in the Swedish Broadcasting Corporation's "News for Consumers" ("Konsumentekot") today, Tuesday July 19th, 1988.

A researcher at the Swedish National Defense Research Institute (FOA) claims that he has found a possible cause for the well known Audi 100 involuntary acceleration phenomena. The researcher, Mats Gunnerhed, active in the field of reliability of technical systems, says that the automatic speed control probably is to blame for many of the accidents. By manipulating just one of the connections on the electronic board that is part of the cruise control function, he has been able to reproduce the unexpected applying of full throttle. It is not necessary for the cruise control to be activated for the

acceleration to happen. It is enough that the main power switch for the automatic speed control is in the "on" position.

Gunnerhed says that the construction as described on the drawings seems good and reliable. A double electronic fault would be required for the involuntary acceleration. However, when the construction was implemented on a physical electronic board a mistake was made that makes it possible for one single electronic fault to cause the unexpected acceleration.

A representative of the cruise control manufacturer, the West German company of HELLA, says that double security is still present since the human error of not applying the brakes is also required for an accident to happen (sic!).

Lars Lindwall, University of Linkoping Computer Center, Sweden.
(LLL@SELIUC51.BITNET)

Bell blames computer error as $4 calls are billed for $400

David Sherman <lsuc!dave@uunet.UU.NET>
19 Jul 88 16:21:46 EDT (Tue)

Toronto Star, July 14, 1988:

OTTAWA (CP) -- Thanks to a computer error, massive long-distance bills have been charged to people in Ottawa who phoned Toronto between May 26 and June 10. Customers were billed the maximum 999 minutes -- or 16 hours, 39 minutes -- for all calls because the computer did not register the signal given when a phone is hung up, Bell says. As a result, a 10-minute call that should have cost $4 would be billed at a whopping $400.

One business, among 83 customers who have already complained, was charged a total of more than $13,000. The average overcharge was $2,450, said Bell spokesman Mary McGregor. Some customers received notices warning that their phone would be disconnected in three days unless they paid up. More complaints are expected when subscribers receive their next bill, McGregor says.

Programming BART (Bay Area Rapid Transit)

Eugene Miya <eugene@amelia.nas.nasa.gov>
Tue, 19 Jul 88 18:25:19 PDT

On a recent climbing trip, the subject of RISKs (this newsgroup) was brought up in discussion with a partner who heads the programming for BART. I passed on the reference to Perrow's "Normal Accidents," which he had read and really enjoyed [and I also told him of various discussions on programming railway systems, note: Bob is English]. Anyway he brought up some interesting points: the current system is only programmed for a maximum of 45 trains (future extensions may require complete reprogramming); BART is a real-time system with 3,000 independent inputs; they use a Yourdon Design Methodology for programming, etc. Oh, yes, he has some interesting stories (like the BART switching yard is not part of BART control, so this nearly led to several

accidents), so we can get some interesting antecdotes if RISKs wants them. Anyways, since Bob is heading back to England this fall and the fact that BART is isolated from any networks (Bob being interested in RISKS), I will agree to act as intermediary for questions about the real-time programming of BART. I will next be seeing Bob in about 2 weeks, so I can batch questions together forward them and an answer if possible. So, if you are interested, and patient, and don't ask things which are too sensitive (security is a concern), I will collect questions. Send them to eugene@amelia.nas.nasa.gov for this purpose (as opposed to my other mail boxes).

eugene miya, NASA Ames

Re: The IRS Illinois Experiment

Michael L. McLean <uiucdcs!pur-ee!mlm@uunet.UU.NET>
Tue, 19 Jul 88 11:55:37 EST

> From: Patrick_A_Townson@unix.SRI.COM
> Subject: The IRS Illinois Experiment
>
> The Internal Revenue Service says it wants to make it faster and easier for
> taxpayers to get their refunds in the future, so it is experimenting with
> a new approach in Illinois during the 1989 tax paying season.

Are you sure about your data? For my 1988 tax return, I went to an H&R block here in Indiana, gave them my signed tax return and $20 .. They sent the return in electronically with the paper backup and my refund arrived in the mail 21 days later. (There was also a 28 day guarantee, if it didn't arrive H&R block returned the $20 fee -- They must put quite a bit of trust in the government system for that one)

The paper backup involved the H&R block person copying the vital numbers from my return onto a different form and sending in my signed return. The possibilities for errors are enormous. I can just see it now the IRS could get three different tax returns from me: my original, the paper backup with a number copied wrong, and the electronic version with a typo.

For an additional cost (don't remember - didn't use this) they had a bank in Maryland loan you your refund and the loan contract explicitly stated that the IRS check is payment. That allows you to get your refund within seven days instead of 28. This also allows the $20+X fee to be automatically deducted from your refund.

Having used this system once, I would use it for refunds again. However after reading risks (and the stupid clerk stories in rec.humor) for awhile I would never authorize the IRS to extract money from my checking account.

I think that a system using PC's would be great, IFF they can make it secure from hackers. The cost to design it properly would be very high, and even then I don't think we can get a safe system developed through the government.

Re: The IRS Illinois Experiment

Lars J Poulsen <lars@ACC-SB-UNIX.ARPA>
Wed, 20 Jul 88 08:45:59 PDT

Patrick Towson's note about the IRS experiment is very interesting.
The projected savings are impressive, but could they be exaggerated ?

The biggest problem is obviously that the email-submitted tax return doesn't have a signature, and thus it could be hard to prosecute people who file fraudulent returns in order to obtain a refund to which they are not entitled. The proposed workaround is to allow filing only through certified tax preparers, who have something to lose if they are caught assisting with such fraud.

The note projects that the IRS would save $63.50 for each electronically filed return, and that the tax preparers would charge $60-$80 on top of their preparation fee. This seems like a lot of money for what would seem like a 10-minute data entry task. I thought data entry jobs paid about $10-$15/hour; double that for G&A overheads, and I get $5/return. Network costs may be another $5, but while these would be a cost to the tax preparers, the IRS would incur them.

Frankly, the whole idea sounds like a P.R. scheme. "Let's get high tech".
I have no doubt that it saves cost to put data on the machine as early in the process as possible, but I thought IRS already did this. Where do these savings come from ?

/ Lars Poulsen

Error rates in barcode data

John Colville <munnari!nswitgould.oz.au!colville@uunet.UU.NET>
Wed, 20 Jul 88 11:32:57 EST

On Monday 18 July, on the ABC's Sydney radio station, 2BL, Margaret Throsby interviewed a representative of a retail organisation about errors in using barcode systems. (Sorry, I don't remember his name or organisation).

The rep. quoted experiments in Adelaide which showed that using barcoding reduced error rates to 5%, compared with earlier experiments in Western Australia where the error rate when individual items were priced was 15%.

He also defined errors in terms of differences between the price charged and the price shown on the shelves. Most of the errors he ascribed to failure of changes to be propagated completely through to the barcode readers i.e. updates not yet done to tapes, tapes not run through, etc.

There is something rather screwy here. I know that we have inflation in Australia of, say 7%, and there are *some* specials from week to week. Even if we assume that the barcode info. is only updated weekly, it seems to me that 5% error rates are way too high.

[If half the errors are `my' way and half are in the store's favour,
should I buy << 40 items every time to avoid errors? :)]

John Colville

PIN on PNB calling card

Nathan K. Meyers <nathanm%hpcvlx@hplabs.HP.COM>
Mon, 18 Jul 88 17:36:45 pdt

What exactly is so irresponsible about Pacific Northwest Bell's encoding charge information into their calling card? It's a credit card -- like all credit cards, it relies on physical security. If someone steals it, or your Visa or Mastercard, he has access to your money. Magnetic stripes on credit cards are pretty common these days -- many of the charge-type phones that accept your calling card will also accept your Visa card.

Your calling card does offer a few security advantages over other credit cards:

1) Nobody can steal your PIN by looking over your shoulder. In other words, no need to "tear the carbons".

2) You can cut your card to ribbons and throw it away, while still enjoying its advantages at almost any telephone in the world. Forget the bulk eraser -- deploy your kitchen shears.

Nathan Meyers, nathanm@hp-pcd.hp.com

Re: Risks of bank ATM cards (more) (RISKS-6.94)

"George H. Feil" <gf08+@andrew.cmu.edu>
Tue, 19 Jul 88 11:08:24 -0400 (EDT)

mordor!lll-crg!lll-winken!ddsw1!karl@rutgers.edu (Karl Denninger) writes:
> o While I was on the phone with Cash Station, Inc. I inquired as to
> the display of balances (this was another "sticking" point with me; they
> were often off by hundreds of dollars). Their reply was that the network
> which interconnects the ATMs "cooks" your balance (!) depending on what
> you do at the terminal. In other words, the balance shown by the terminal
> MAY NOT BE YOUR TRUE BALANCE. When I asked as to why there was no
> indication anywhere that these numbers were "finagled" they indicated that
> the response time of the member bank's computers was insufficient to get a
> real balance.... sounded (and still sounds) fishy to me. Isn't this
> *literally* fraud, as they claim that number on the screen to be your
> BALANCE? (along this line, the machines do not dispense receipts on
> balance inquiries either -- perhaps to prevent you using these as
> "evidence".)

I've been screwed by having bogus balances given by ATM's before.

When I had an account with Mellon Bank (which, in my opinion, is run by a bunch of weasels for many reasons), the balances which appeared on my receipts were often as much as 48 hours behind transactions that already occurred. So, in thinking that I had plenty in my account, I would make a withdrawal, only to have the bank charge me $20 for overdrafting my account. They admitted that the balances weren't always accurrate, and cannot be trusted. Of course, they don't tell you that when you apply for the card...

Another possiblity is when the bank's computer is down. Sometimes, the network simply refuses to allow me access to my funds. But at other times, I was allowed to make a withdrawal, but my account balance was "unavailable".

It makes me wonder how much banks have made by suckering customers into believing that they have more funds in their account then they actually have, and having them unknowingly overdraw on their accounts?

From now on, I always keep the receipts, and balance the account on my own. My suggestion: never trust the balance figure that the ATM prints out.

George H. Feil (HAL)

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 26

Saturday 23 July 1988

Contents

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

Misuse of the UK Data Protection Act

Brian Randell <Brian_Randell%newcastle.ac.uk@NSS.Cs.Ucl.AC.UK>
Thu, 21 Jul 88 11:29:20 WET DST

RISKS readers are all too used to learning of new ways in which the power of computers has been creatively misused. This posting, however, concerns misuse of a law which was itself in part intended to prevent computer misuse!

One of the provisions of the UK Data Protection Act, which is now in force, enables individuals to have the right to obtain copies of information held about them in computers (excepting by the security organisations, etc.). An article in the 21 July 1988 issue of Computing reveals that the Act is being abused by employers who are using it to check up on prospective employee's backgrounds. It quotes the fourth report of the Data Protection Registrar as complaining that:

> "Employers are using the Act as a back door for getting an individual's record, and this is wrong... To use the Act to force individuals to find and reveal information about themselves is contrary to the objectives of data protection and should be stopped."

The article explains that this misuse is most common by local authorities checking up on taxi drivers prior to granting trading licenses, It quotes the Assistant data protection registrar:

> "Individuals are in a difficult position as they want the job and are not too keen to stand up for their rights ... the problem is that minor offences, which under the Rehabilitation of Offenders Act no longer count against an individual, still appear on police records."

Apparently it will take a change in the law to make it illegal for someone to be forced to exercise his rights under the Data Protection Act.

Brian Randell, Computing Laboratory, University of Newcastle upon Tyne

JANET = Brian_Randell@uk.ac.newcastle
UUCP = ...!ukc!newcastle.ac.uk!Brian_Randell PHONE = +44 91 232 9233

Risks of not running new software in parallel with old

Jon Reeves <reevesdecvax.dec.com>
Wed, 20 Jul 88 21:05:42 EDT

Regular readers have probably heard stories like this before, but it's worth repeating.

The Bill's in the Mail [Corporate Report Minnesota, July 1988; by Lee Schafer]

Mona, Meyer & McGrath, the Bloomington [Minnesota] public relations firm that placed 470 on the 1987 Inc. [magazine] 500 list of fastest growing companies, is still feeling the effects of a no-growth course of action that it unwittingly adopted late last year and early this year.

It all started last summer when Mona, Meyer decided that it had outgrown its accounting and billing system, which, according to partner Scott Meyer, was suited to a company with $1 million in annual revenue, rather than the $5 million company Mona, Meyer had become. ... The partners ... decided to hire a Dallas firm, Data Directions Inc., to create a custom system.

In October 1987, the software firm figured the necessary work was completed, but advised Mona, Meyer to continue to run the old system--just in case. This advice was ignored. "We decided to pull the plug on the old system and flip the switch on the new one," Meyer says. The intent was to save some staff time by running a single system. "Well, we flipped the switch and it didn't work."

October, November, and December billings went uncompleted while Mona, Meyer scrambled for solutions. October and November bills were finally mailed in

January, but they were prepared by hand. Only by mid-March did the system work well enough to allow a combined January and February billing to be mailed.

As one might expect with ceased income but continued outgo, Mona, Meyer faced a cash-flow crunch by mid-January. ... Meyer says bank loans carried the firm until the billing situation was straightened out. Although phones weren't ringing off the hook with clients wondering about their bills, a few customers were unhappy with the situation because they had to pay for 1987 services out of 1988 budgets.

Jon Reeves

Computer Error causes bills to be mailed to wrong address

Todd Medlin <medlin@csclea>
Thu, 21 Jul 88 18:23:07 edt

Local radio stations (in the Research Triangle Park, NC area) carried a story this morning concerning incorrect billing to students at NC State. It seems that the program used to generate bills would correctly generate a student's bill, but, then address it to the wrong student. The problem was discovered only after 6000 bills were mailed to the wrong students.

Penetrating the Phone System

the tty of Geoff Goodfellow <geoff@Fernwood.MPK.CA.US>
Fri, 22 Jul 88 09:39:16 PST

PERSONAL COMPUTER USERS PENETRATING NATION`S TELEPHONE SYSTEM
By JOHN MARKOFF with ANDREW POLLACK (c.1988 N.Y. Times News Service)

NEW YORK - Sophisticated personal computer users are becoming increasingly adept at penetrating the nation's telephone system, raising questions about the security and privacy of the phone system, industry experts and law enforcement offiials say. The vulnerability of the phone system to such tampering has grown significantly in the past decade or so as telephone companies have largely replaced electro-mechanical call-routing equipment with computer-controlled switches.

As a result, people with the expertise can illegally connect their personal computers to the phone network. With the proper commands, these intruders can do such things as eavesdrop, add calls to someone's bill, alter or destroy data, have all calls to a particular number automatically forwarded to another number or keep someone's line permanently busy, it was disclosed in an internal memorandum written by a manager of electronic security operations at the San Francisco-based Pacific Bell Telephone Co. and in interviews with company officials.

Peter Neumann, a computer security consultant at SRI International Inc. in Menlo Park, Calif., said telephone companies are only beginning to awaken to the security problems created by the increasing computerization of the telephone network. ``As far as our vulnerability, we all have our heads in the sand,'' he said. ``We have to redefine our notions of what we entrust to

computers and to communication networks.''

Some personal computer enthusiasts, often called ``hackers,'' view the task of breaking into the telephone system as a test of their skills and only infrequently inflict damage, industry officials and consultants say. But others act with criminal intent.

In his memo, the Pacific Bell security manager also warned that an electronic intruder could essentially disable an entire central switching office for routing calls, disrupting telephone service to entire neighborhoods. Furthermore, he said, organized-crime groups or terrorists might use such technology to their own advantage.

The integrity of customer bills could also be compromised, he said. Customers might rightfully or wrongfully dispute expensive calls, claiming the calls were placed on their bills by computer hackers.

Earlier this month, a teen-age computer enthusiast who requested anonymity provided The New York Times with the Pacific Bell memo, which was written a year ago. He said it had been obtained by a fellow hacker who illicitly eavesdropped on a facsimile transmission between Pacific Bell offices in San Francisco. The memo, which Pacific Bell verified as authentic, concluded that ``the number of individuals capable of entering Pacific Bell operating systems is growing'' and that ``computer hackers are becoming more sophisticated in their attacks.''

In one of two cases cited in the memo, a group of teen-age computer hobbyists were able to do such things as ``monitor each other's lines for fun'' and ``seize another person's dial tone and make calls appear on their bill,'' the memo said. One of the hackers used his knowledge to disconnect and tie up the telephone services of people he did not like. In addition, ``he would add several custom-calling features to their lines to create larger bills,'' the memo said.

In the second case, police searched the Southern California home of a man thought to be breaking into the computers of a Santa Cruz, Calif., software company. They discovered the man could also gain access to all of Pacific Bell's Southern California switching computers. wFiles were found containing codes and employee passwords for connecting with -- or ``logging on to'' -- the Pacific Bell switching systems and related computers. The man also had commands for controlling the equipment.

In another case involving tampering with telephone company switching equipment, local police and the FBI in the San Francisco area are investigating Kevin Poulsen, a former programmer at Sun Microsystems, said Joseph Burton, an assistant U.S. attorney in San Jose, and John Glang, a deputy district attorney for San Mateo County.

Authorities searched Poulsen's apartment in Menlo Park in February as well as the residence of a suspected accomplice in San Francisco, the officials said. Poulsen was said to be in Southern California and was unavailable for comment.

Burton said he could not discuss a current investigation. Glang would say only that the case had been taken over by the federal government because ``there are some potential national security overtones.'' But a security expert familiar with the case, who requested anonymity, said that Poulsen ``pretty clearly demonstrated you can get in and romp around inside a Bell operating system.'' ``What it pointed out,'' he said, ``was the serious vulnerability.''

Security consultants said other phone companies are equally vulnerable to such breaches. They noted that most phone service in the nation is provided by companies that were part of the Bell System until it was broken up in 1984 and still use similar equipment and procedures.

Michigan Bell officials said they had caught an intruder who tampered with the company's switching equipment last year. A spokesman declined to give details of the incident but said no arrest was made. ``We have been able to tighten our security arrangements,'' said Phil Jones, a company spokesman. ``There were lessons to be learned here.''

Jack Hancock, vice president for information systems at Pacific Bell, said his company had also taken steps to make it tougher to penetrate its systems. He said, however, that the company had to strike a balance between security and cost considerations so the phone system would still be widely affordable and easy to maintain.

``We could secure the telephone system totally, but the cost would be enormous,'' he said. ``A public service will probably always have certain insecurities in it.''

Though Pacific Bell refused to disclose the security measures it had taken, the company said it had restricted the ability to dial into its computers from remote points.

As computerized communications become more sophisticated, companies will be able to improve security at a reasonable cost, said Barry K. Schwartz, a systems planning manager at Bell Communications Research, which does research for the seven Bell operating companies. It will be increasingly possible to program a computer so it will only answer a call from an authorized phone, he said. Another new technology on the horizon, he said, is electronic voice verification. A security system using this technology would be able to recognize those authorized to gain access to a computer by their voice patterns.

Telephone companies have long had to worry about electronic abuse of their networks. For several decades individuals have used electronic equipment to make long-distance phone calls for free. Some have used devices that generate a series of tones that provides access to long-distance lines. Telephone companies have installed equipment on their lines to detect and thwart such abuse. In other instances, people have used personal computers to find long-distance access codes belonging to other users. They do this by programming computers to keep trying various numbers until they hit upon one that works. But while costly, these kinds of abuse are not much of a threat to the integrity of the system because they do not affect the system itself.

The new problems involving network tampering are arising, experts say, because the switches that route calls are now mostly electronic, meaning they are essentially big computers. If a customer wants an option like call forwarding or call waiting added to his or her telephone service, that is done by typing commands into a computer, not by moving wires and switches.

Pacific Bell said 79 percent of its customers are now served by computerized switching systems. Experts say these electronic networks are especially vulnerable to tampering because it is possible to dial up the computers controlling the switches from the outside. Phone companies designed their systems this way to make it easier for them to change the system and diagnose problems. For example, a technician in the field trying to diagnose problems on a line needs to be able to dial certain test circuits in the central office. But such a dial-up capability can also be used by outsiders with personal computers and modems who know the proper numbers to call and the proper procedures to get on the system.

The ability to eavesdrop on telephone calls is included in the system to allow an operator to check to see whether a line that is busy for a long time is being used or whether the phone is off the hook or the line is broken.

One security consultant who requested anonymity said this capability had also made it much easier for law enforcement officials to wiretap a line. When the police receive court permission to conduct a wiretap, they can have the phone company dial up the switch serving the line so conversations can be monitored from a remote location. Obtaining the information needed to break into the phone system can be difficult, but intruders often do it by impersonating phone company employees -- a practice that hackers call ``social engineering.''

A teen-ager interviewed by Pacific Bell officials after his arrest told investigators that he had entered a number of Pacific Bell facilities in the San Francisco area disguised as a Federal Express delivery man in order to search for manuals and other documents, according to the company memo. The youth also said he had impersonated telephone security officials to obtain passwords and other information.

Electronic IQ Testing

Stephen Colwill <mcvax!praxis!steve@uunet.UU.NET>
Thu, 21 Jul 88 9:58:09 BST

People interested in scenarios arising from the possibility of mechanised IQ testing might like to read `Player Piano' by Kurt Vonnegut. I say no more!

Re: IRS and Electronic Filing

ASTROBOY <LI.BOHRER@A20.CC.UTEXAS.EDU>
Fri 22 Jul 88 00:59:28-CDT

Lars Poulson writes (regarding the IRS Tax return proposal):

>The note projects that the IRS would save $63.50 for each electronically filed
>return, and that the tax preparers would charge $60-$80 on top of their
>preparation fee. This seems like a lot of money for what would seem like a
>10-minute data entry task. I thought data entry jobs paid about $10-$15/hour;
>double that for G&A overheads, and I get $5/return. Network costs may be
>another $5, but while these would be a cost to the tax preparers, the IRS woul
>incur them.

I don't know where you got your information about what data-entry pays, but, at least in the Austin TX job market, you're off by as much as 300%. Data entry clerks (the key word here is `clerks') at the IRS facility here start at $4.65/hr and all you need is a high school diploma. This salary is true of the market in general. (I have checked.) Wendy's starts at $4.25/hr, for crying out loud, and you don't even need a *brain* to work there.

The biggest advantage in having a tax preparer file your return electronically is that you will circumvent the underpaid, overworked, slightly addled civil servant and can be reasonably sure that the numbers were correctly entered. If you send in your paper from, and the caffeine-crazed/caffeine-depleted drone enters the numbers incorrectly, you then have to deal with the Tax Examiner. They are paid the premium salary of $5.50/hr, and need a college degree for that. Needless to say, these

jobs do not garner the nation's best.

Bill Bohrer

Re: The IRS Illinois Experiment

<mnetor!utzoo!henry@uunet.UU.NET>
Fri, 22 Jul 88 20:31:58 EDT

>... Where do these savings come from ?

The key point is that money that used to come out of the IRS budget now will come out of yours. This is why the IRS is big on the idea. The question is whether they can make it attractive enough to sell it.

Henry Spencer @ U of Toronto Zoology

Re: "Man in the loop"

Will Martin -- AMXAL-RI <wmartin@ALMSA-1.ARPA>
Tue, 19 Jul 88 15:51:22 CDT

> The July 18 Los Angeles Times carries an op-ed piece by Peter D. Zimmerman
> ... But the real lesson from the tragedy in the Persian Gulf is that
> computers, no matter how smart, are fallible. Sensors, no matter how
> good, will often transmit conflicting information. The danger is not
> that we will fail to prepare the machines to cope with expected situa-
> tions. It is the absolute certainty that crucial events will be ones
> we have not anticipated.

I would have a lot more respect for Mr. Zimmerman if he had added the line,

" -- and that people, too, no matter how smart, are fallible."

to the first sentence above. GIGO applies not only to computers but to humans, except that we are complex enough computing devices to often perform unconscious "sanity checks" that we probably would fail to implement in software.

After all, there WAS a "man in the loop" on the Vincennes -- the computers did not automatically fire the missiles without human intervention.

Will Martin

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 27

Monday 25 July 1988

Contents

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

A Fishy Story

John Colville <munnari!nswitgould.oz.au!colville@uunet.UU.NET>
Mon, 25 Jul 88 16:23:31 EST

From "The Sydney Morning Herald", 23 July 1988 (Reprinted without permission)

The new restaurant at the Opera House seems to be having a few technical troubles. Three people lunching there yesterday ordered river trout. Some minutes later, an embarrassed waiter told them: "Sorry, we put the trout

through the cash register, and it came out in the kitchen as octopus." The diners settled for octopus anyway.

John Colville

[Obviously the wrong "menu" popped up on the screen! Or were they pulling somebody's leg (not the octopus') and using the computer as an excuse? PGN]

Inconsistent Data Taxes Vancouver Woman

Don Chiasson <G.CHIASSON@DREA-XX.ARPA>
Mon, 25 Jul 88 16:44:30 ADT

From the Toronto Globe and Mail, page 3, July 25, 1988 (Canadian Press), as usual without permission:

BC Woman Alive And Well Despite What Taxman Says

Judi Sommer insists she is alive and well and living in Vancouver. But the 40 year old has trouble convincing the taxman of that.

"They say their computer has me down as officially dead but gainfully employed," she said during the weekend.

Ms Sommer said the dilemma is preventing her from collecting the $1,200 she expects back from Revenue Canada.

"What do I have to do to prove I'm alive?" the teacher asked.

Her troubles started in 1986 when her mother, Mollie, died. A mixup in her lawyer's office led to the placing of Ms Sommer's social insurance number on her mother's death certificate.

She said that, when she asked a Revenue Canada official last year if her tax forms had been received, he told her the social insurance number she gave belonged to a dead person.

It took three months for her to sort out the problem and get her 1986 tax refund ... But she said she is now facing the same problem with her 1987 return.

Revenue Canada spokesman Harm Dhillon acknowledged that mistakes are made occasionally, but added that he has never heard of someone being both dead and gainfully employed at the same time in his 11 years with the tax office.

Ottawa has promised to straighten out the mistake and forward Ms Sommer her refund.

Computer Viruses and RETROVIRUSES (Re: RISKS-7.23)

Peter J. Denning <pjd@riacs.edu>
Sat, 23 Jul 88 14:10:53 pdt

Peter Neumann asked what terminology could be applied to the corrupted data that propagated through a system or network. The closest biological analogy is the retrovirus. A retrovirus (such as the HIV, or human immunodeficiency virus, or AIDS) incorporates itself into the genetic material of the cell that it attacks, causing the cell to alter its function; the reproductive processes of the cell spawn new copies of the retrovirus. The retrovirus is not capable of self-reproduction. So Neumann's ARPANET node "data virus" is

analogous to a retrovirus.

But let's be careful about the analogies with biology. They are intriguing metaphors that give the appearance that our machines have lives of their own, and absolve us of the responsibilities for their behavior.

Peter Denning

Hacking central office switches - too easy? [See also RISKS-7.26]

"John T. Powers Jr. (Jac" <POWERS@ibm.com>
23 Jul 88 00:08:58 PDT

I read a New York Times article in the San Jose Mercury-News for Friday, 7/22/88 which spoiled my day. The title was fairly routine: "Computer users break privacy, security of phones". Being mildly interested in security, I read it anyway.

If this article is correct, crackers have been playing games with Pacific Bell central office switches up to no less than a year ago, maybe even now. It appears that open modems were left on what I would call "console" ports, allowing crackers access to operator-class commands after guessing or otherwise obtaining passwords. Once logged on, "visitors" could reportedly disconnect a line, assign it to another account ("steal dial tone"), and who knows what other mischief.

It would have been easy for them to make this kind of activity much harder than it evidently was. A simple callback system (something I introduced at IBM about 10 years ago, and common now) would, if used correctly, make it *much* harder to gain unauthorized access to a CO switch. In addition, it would probably warn of interest by unauthorized persons. Today, much more sophisticated security systems are not only available but cheap.

It amazes me that a phone company, of all possible victims, would omit such a simple and effective barrier to mischief. It would have cost them almost nothing. I've toured a number of Pacific Bell COs, and their physical security looks pretty good to me. It's almost *inconceivable* to me that that they would leave a back door open via, of all things, the bleeping *telephone*.

Anyone know how accurate this report is, and what PacBell did about it, if true?

Does this remind you of another recent security horror story?

Disclaimer: These are my views only... and even I might disclaim them later.
Jack Powers IBM Almaden Research Lab powers@ibm.com
Flames at 1200bps or less to 408/779-7472. Voice: 408/927-1495. Share water.

"Man in the Loop"

<WHMurray@DOCKMASTER.ARPA>
Tue, 19 Jul 88 09:31 EDT

Rodney Hoffman offers:

> >Despite the fact that the Aegis system has been exhaustively tested at the
> >RCA lab in New Jersey and has been at sea for years, it still failed to make
> >the right decision the first time an occasion to fire a live round arose.

It is clear that the first time that it hit a target, it was a friendly target. What evidence is that this is the first opportunity, or even the first round? [I also question "exhaustively." One of the problems of this class of system is that they do not permit of exhaustive testing.]

[As did Will Martin (RISKS-6.26), Bill noted that "People are fallible". PGN]
Still, they are less fallible in an anticipatory mode than they are in a life and death crisis situation.

Bill Murray

AEGIS

Herb Lin <LIN@XX.LCS.MIT.EDU>
Sun, 24 Jul 1988 07:26 EDT

For more commentary on AEGIS and SDI, you might find an article in Scientific American interesting -- December 1985, on computer software and SDI. It contains a description of the early operational testing of AEGIS (including defects in the testing), and draws comparisons to SDI.

Journal of Computing and Society

Gary Chapman <chapman@csli.stanford.edu>
Sun, 17 Jul 88 10:59:33 PDT

CALL FOR PAPERS for THE JOURNAL OF COMPUTING AND SOCIETY

P.O. Box 717, Palo Alto, CA 94301, (415) 322-3778

The Journal of Computing and Society will begin publishing in late 1988. It will be a quarterly journal of material on the social implications of computing technology and computerization. The journal is soliciting articles on computers and privacy, computers and war, computers and power relations, computers and gender, computers and politics, computers and social theory, and similar subjects.

The deadline for the Spring 1989 issue is September 15, 1988.

The emphasis in this journal will be on high quality writing and provocative ideas. Original research is welcome, but the journal will try to avoid conventional academic writing in favor of well-crafted essays. The journal is intended to appeal to a general audience as well as the profession of computer

science. Preference in publication will be given to material showing originality, creativity, relevance to substantive problems in society, and readability. There will be no political or philosophical prejudice--all viewpoints are welcome.

The Journal of Computing and Society is edited by Gary Chapman, executive director of Computer Professionals for Social Responsibility. Questions regarding manuscripts should be directed to him at the address above.

Manuscripts should be submitted in quadruplicate, typed or laser-printed, on 8 1/2" x 11" paper with one-inch margins all around. The Journal's style will be the same as that of The Chicago Manual of Style and The Communications of the ACM.

The editorial board of the Journal of Computing and Society consists of the following people: Jerry Berman; Margaret Boden; David Burnham; Hubert Dreyfus; Jean-Louis Gassee; Calvin Gotlieb; Douglas Hofstadter; Deborah Johnson; Rob Kling; John Ladd; Abbe Mowshowitz; Peter G. Neumann; Susan Nycum; Kristen Nygaard; Paul Saffo; Mike Sharples; Lenny Siegel; Luca Simoncini; Brian Smith; Lucy Suchman; Zhisong Tang; Joseph Weizenbaum; Alan F. Westin; Langdon Winner; and Terry Winograd.

Subscription rates for The Journal of Computing and Society have not yet been determined, but there will be a personal subscription rate for individuals.

The Journal of Computing and Society will be published by Ablex Publishing Corporation of Norwood, New Jersey.

Barcodes (re: RISKS-7.13)

Jerome H. Saltzer <Saltzer@ATHENA.MIT.EDU>
Fri, 22 Jul 88 14:37:04 EDT

> From: dap@cgl.ucsf.EDU (David A. Pearlman)
> Subject: Grocery Store Barcodes: Another game you don't win
> All this talk about how ATM's don't make mistakes in the customer's
> favor reminds me of one of my pet peeves: When the price on the food
> shelf is not the same as the price scanned at the cash register.

This is a case in which a combination of technology and store policy can make a big difference. The last Albertson's store in which I shopped had a voice synthesizer that announced the price of every item scanned, and a big sign saying that if the price scanned isn't identical to the price on the shelf you get the item for free.

Jerry Saltzer

The IRS Illinois Experiment

<LENOIL@XX.LCS.MIT.EDU>

Mon, 25 Jul 1988 14:19 EDT

One way to partially automate the filing process without granting online access to IRS computers to the masses would be to supply a tax filing program to taxpayers and allow them to file on floppy disk. The cost would be more than direct electronic filing, but should be less than a paper return.

"Scratch-and-win"? Try "X-ray-and-win"! [RISKS-7.13]

Fred Baube <fbaube@note.nsf.gov>
Fri, 01 Jul 88 14:40:53 -0400

Even if they make instant-win lottery cards immune to non-destructive testing by X-ray, aren't there small CAT scanners or NMR imagers out there that can determine the location of ink molecules, providing the same winner/no-winner information ?

PIN on PNB calling card

Mark Mandel <Mandel@BCO-MULTICS.ARPA>
Thu, 21 Jul 88 16:48 EDT

Agreed, the calling card with magnetically-encoded PIN is similar to a credit card, though a credit card still provides a security barrier of sorts in the signature. But according to the description we were given, PNB doesn't tell you so. What started this discussion was someone's report of PNB's form letter accompanying the mailed card, in which they said,

a: For security, don't write your PIN on your card or keep it in the wallet, and
b: You don't even need to remember your PIN because the card encodes it!

We who read this digest recognize the contradiction here, but we're not typical consumers. The PINheads who set up that arrangement and wrote the letter don't seem to see that (a) is no protection in light of (b). How can Jane and Joe Average be expected to see it? Pacific Northwest Bell's irresponsibity lies not so much in mag-encoding the PIN, per se, as in failing to inform the card's users of the resulting risk, and in actually disguising this risk by warning them to keep the PIN separate from the card.

-- Mark Mandel

* My employer is not responsible for anything I say, think, do, or eat.

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 28

Tuesday 26 July 1988

Contents

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

Pentagon testing (an oxymoron) (Re: RISKS-7.24)

Mike Trout <miket@brspyr1.brs.com>
25 Jul 88 21:21:13 GMT

In article <12415398632.18.NEUMANN@KL.SRI.COM>, Gary Chapman writes:

> Subject: Aegis testing data withheld from Congress
> Defense Week reports that an unclassified report of the General Accounting
> Office (GAO) reveals that the Navy withheld testing problems of the Aegis
> air defense system from the Congress. "Personnel and Aegis equipment were
> not subjected to targets or tactics that would be found in combat," ...

This is typical of Pentagon testing, and seems to be particularly prevalent in the Aegis system. An interesting parallel concerns the testing for the Phalanx close-in shipboard missile defense system, which of course is included as part of the Aegis umbrella. The Navy's final results of the testing conducted for Phalanx reported that the system had achieved greater than 80% "success." But

what was the definition of "success?" Pentagon watchdog groups did a little digging with the Freedom of Information Act, and determined that "success" had been interpreted as "destruction of the incoming missile." Well, that seemed okay, so most investigations were dropped. But some whistle-blowers in the Pentagon produced some disconcerting information. While it was true that simulated incoming missiles had indeed been "hit" and "destroyed," it had been determined that the debris and rocket fuel of the destroyed missile would continue onward and hit the ship, causing tremendous impact and an inevitable fire. It was estimated that this would be enough to destroy or knock out nearly any vessel. But since the simulated missiles had been "destroyed," the Navy proudly announced that Phalanx had passed the test. Empirical evidence from the Falklands war makes the Phalanx testing look even less realistic. Only one of the Exocets hitting Royal Navy ships exploded, yet the dud Exocets still did hellish damage, including sinking two ships. It also appears that the missile that hit the USS _Stark_ did not go off.

Another example uncovered by the Dina Rasor group: A mobility/breakdown test was conducted for the new M-1 Abrams tank. The tank failed the test. The test was run again, with identical results. The Aberdeen Proving Grounds was instructed to just keep running the test until the tank passed. On the 161st try, the tank passed the test. The testing information provided to Congress included only that which pertained to the 161st test; the previous 160 tests were not even mentioned.

Rasor has also uncovered suspicious changes in the testing for both ALCM and GLCM (Air- and Ground- Launched Cruise Missiles). Recent stories of doctored test results for the Rockwell B-1B are similar.

In any system in which hardware or software is to undergo a realistic test, it is critical that ALL test results be released, unaltered. Any other course of action changes the test from a realistic simulation to a public relations gimmick. In the case of software written for a computer game, the results of doctored testing may be comical. In the case of a military weapon, the results may be disastrous.

Michael Trout (miket@brspyr1) =-=-=-=-=-=-= UUCP:brspyr1!miket
BRS Information Technologies, 1200 Rt. 7, Latham, N.Y. 12110 (518) 783-1161

Re: "Man in the Loop"

Rodney Hoffman <Hoffman.es@Xerox.COM>
26 Jul 88 07:38:52 PDT (Tuesday)

I recently posted excerpts from Peter Zimmerman's article about AEGIS and Star Wars and the "man in the loop". Just in case it wasn't clear, all but the lead introductory sentence of that was from Peter Zimmerman, not directly from me. Anyone wishing a copy of his complete article may contact me.

I completely agree with Will Martin and Bill Murray when they each insisted on adding to Zimmerman's piece a stronger statement about HUMAN fallibility.

In my initial posting, I thought I would let Zimmerman speak for himself. In

light of the responses, I probably should have appended my own reactions. In particular, I believe many lessons implicit in Zimmerman's piece (and familiar to all RISKS readers) are well-taken. Among them:

* The blind faith many people place in computer analysis is rarely justified. (This of course includes the hype the promoters use to sell systems to military buyers, to politicians, and to voters.)

* Congress's "man in the loop" mandate is an unthinking palliative, not worth much, and it shouldn't lull people into thinking the problem is fixed.

* To have a hope of being effective, "people in the loop" need additional information and training and options.

* Life-critical computer systems need stringent testing by disinterested parties (including operational testing whenever feasible).

* Many, perhaps most, real combat situations cannot be anticipated.

* The hazards at risk in Star Wars should rule out its development.

Rodney Hoffman

NOVA on risks of fighter technology

Dave Curry <davy@intrepid.ecn.purdue.edu>
Mon, 25 Jul 88 16:59:49 EST

WTTW (Channel 11), the Chicago PBS station, showed a commercial last night for a NOVA episode on the risks of fighter plane technology. The preview blurb mentioned questions like is there too much data for the pilot to keep track of, are G's too great, etc.

I would assume other PBS stations will have this episode at some point also (I'm not a regular watcher of PBS or NOVA, so I don't know how they work). WTTW is showing it on Tuesday 7/26/88 at (I believe) 9pm EDT.

--Dave Curry, Purdue University

---

re: Hacking central office switches

<Laura_Halliday@mtsg.ubc.ca>
Mon, 25 Jul 88 14:30:38 PDT

John T. Powers Jr. writes (Risks 7.27):

> It would have been easy for them to make this kind of activity much harder
> than it evidently was. ...

When I worked for BCTel, we had an even simpler solution: remote access to

the console was over dedicated lines. Grossly unsophisticated, but effective.

laura halliday laura_halliday%mtsg.ubc.ca@um.cc.umich.edu

Law student sues micro sysop under ECPA

John Gilmore <hoptoad.UUCP!gnu@cgl.ucsf.EDU>
Mon, 25 Jul 88 22:09:35 PDT

This appeared in a recent FidoNews (comp.org.fidonet on Usenet). The FidoNet is a few thousand IBM PC's all calling each other over dialup lines; similar to Usenet; less flexible; evolving faster.

> Copyright 1988 by the International FidoNet Association. All rights reserved. Duplication and/or distribution permitted for noncommercial purposes only. For use in other circumstances, please contact IFNA at (314) 576-4067. IFNA may also be contacted at PO Box 41143, St. Louis, MO 63141.
>
> FidoNews 5-30 Page 3 25 Jul 1988
>
> Jonathan D. Wallace, Esq.
> 1:107/801
>
> SYSOP LIABILITY FOR DISCLOSING PRIVATE MESSAGES
>
> In what appears to be the first case of its kind, an Indiana law student and BBS user has sued a local sysop, Bob Predaina, in federal court, claiming that he intentionally disclosed her private electronic mail to others without her permission.
>
> The lawsuit, which is in the early stages and has not reached trial, relies upon the Electronic Communications Privacy Act of 1986 (the "ECPA"), which makes disclosure of private electronic mail without consent either of the sender or the recipient a federal crime.
>
> The ECPA does not obligate sysops to offer private mail on their systems. However, if a sysop promises private mail, that promise must be kept and the contents of private messages may not be disclosed without consent.
>
> The ECPA provides limited exceptions to the general rule of no disclosure. A sysop may voluntarily disclose to law enforcement authorities the contents of a message pertaining to the commission of a crime, if read inadvertently by him or if it is read pursuant to the exercise of his duties as a sysop.
>
> Until the courts clarify these rules, sysops who read private mail on their systems and disclose it may be playing with fire. Prior court cases involving telephone operators have established

some useful guidelines: an operator may disclose information she overheard while checking the line at the user's request, but may not disclose information overheard while eavesdropping out of curiosity. Sysops, like phone operators, will not be considered to have a blanket authorization to intercept and disclose private messages.

Systems such as Fido 11w which routinely make all private mail visible to the sysop are therefore problematic. BBS programmers should consider making private mail truly private--while allowing sysops to turn the private mail option off if they do not want it.

In the meantime, sysops should reconsider whether it is worth having private mail on their systems and should make clear to users in no uncertain terms, through bulletins and messages, the degree of privacy which can be expected, if any.

Note: a copy of the complaint filed in the Thompson v. Predaina case is available on the LLM BBS, Fido 107/801 (212)766-3788) in file area 5 under the name "Indiana".

* * *

JONATHAN D. WALLACE, ESQ. is an attorney in New York City specializing in computer law. With Rees Morrison, he is the author of the Sysop's Legal Manual, published this year by LLM Press. He can be reached at (212) 766-3785 (voice) or at the LLM BBS, given above.

- -

The same issue of FidoNews also contains a relevant ad:

SYSOP LEGAL MANUAL FOR SALE

SYSLAW, the Sysop's Legal Manual,
by Jonathan D. Wallace Esq. and Rees Morrison Esq.

This 130 page book, newly published by LLM Press, includes chapters on the Electronic Communication Privacy Act, sysop liability for illegal uploads such as pirated software and stolen credit card codes, libel and state computer crime laws. The book is $21.00 (includes postage and handling) from LLM Press, 150 Broadway Suite 610, New York, New York 10038. New York residents include 8.25 percent sales tax.

[This item is included in RISKS because the book might just answer questions that have been raised here repeatedly. This notice represents no endorsement of the book, and is for your information only. On one hand, much of the cited information is publically available. On the other hand, its compilation and interpretation in one place might be useful -- assuming the book is accurate. If this redistribution in RISKS can in any way be deemed in violation of the

FidoNet banner above, then perhaps FidoNet itself was in violation of its own noncommercial dictum. By the way, RISKS is unquestionably a noncommercial effort, in case you hadn't noticed. PGN]

Scanning instant-win lottery cards (Re: RISKS-7.27)

Rich Kulawiec <rsk@payton.cc.purdue.edu>
Tue, 26 Jul 88 01:43:27 EST

Fred Baube <fbaube@note.nsf.gov> writes:

"Even if they make instant-win lottery cards immune to non-destructive testing by X-ray, aren't there small CAT scanners or NMR imagers out there that can determine the location of ink molecules, providing the same winner/no-winner information ?"

CAT scanners also use X-rays to produce an image, so a card immune to "peeping" by a conventional X-ray machine is very likely to be immune to a CAT scanner as well. (All that is necessary for this is that the inked area have the same absorption cross-section as the non-inked area.) A similar comment applies to ultrasonic imaging techniques. NMR imaging might reveal the hidden print, if the ink molecules are distinguishable from those non-ink molecules around them. My (very casual) guess is that using an area that's written in two shades of ink with slightly differing formulations might defeat this approach; i.e. if both areas consist of a substance with nearly the same chemical composition and structure, they may be indistinguishable via NMR.

Rich Kulawiec

Wanted: Info on Ergonometrics

Emily S. Bryant <dartvax!eleazar!emilyb.UUCP@seismo.css.gov>
25 Jul 88 18:42:52 GMT

I am posting the following for a colleague; please send responses by mail to:

michael.whitman@dartmouth.edu or ...{decvax, ihnp4}!dartvax!michael.whitman

and NOT to me! Thanks. Emily Bryant.

WANTED: Information on how to set up a computer workstation's screen, keyboard, and seating to minimize eyestrain and physical fatigue.

I am interested in any research results which pertain primarily to eye- and backstrain, but am not looking for information on possible effects of video display terminals on pregnant operators.

I am looking for recommendations on

1) Worker's height : chair in inches;

2) Distance from eyes to computer screen;

3) Angle from eye level to center of screen;

4) Height of keyboard above lap level;

Also,

5) Do higher screen resolution and refresh-rate reduce eyestrain?

6) Is it personal preference or documentable fact that black letters on "white" background (Macintosh), green on black, amber on black, or some other combination, are easier on daylong viewers' eyes?

8) What kind of ceiling fluorescent bulbs help reduce eyestrain?

9) What kind of chairs help minimize backstrain?

Finally, how about common sense suggestions in addition to these:

10) Workers should look away periodically from their screens and focus on objects in the distance;

11) Use a screen font which is large enough to be read easily;

12) Use eyeglasses when computing for long hours, with a prescription specifically for one's actual eye-to-screen distance.

I am researching a feature article for a publication at Dartmouth College. Since I have been able to find no recent articles on this except a NY Times 6/23/88 article, I hope suggestions for information sources will be sent.

Michael Whitman
Dartmouth College

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 29

Wednesday 27 July 1988

Contents

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

Comparison of hazards

<attcan!utzoo!henry@uunet.UU.NET>
Wed, 27 Jul 88 14:04:40 EDT

> * The hazards at risk in Star Wars should rule out its development.

Grace Hopper gave a talk here some years back in which she made a point that is relevant to this discussion, and more generally as well. I forget the details, but she was in some bureaucratic situation where she was required to take correspondence courses in *something*, and most of the possibilities were ruled out because she was ineligible or had already taken them... so she ended up taking War College courses, intended for training admirals and such. One of the exercises was to plan an invasion of an island, given some details on overall situation, available manpower, etc. Actually, that was

just the first part of the exercise. The second part was "What would be the consequences if your plan failed?". The third, and most relevant, part was "What would be the consequences of not attempting this plan?". (Her comment was that she'd seen many plans for information systems, very few of which attempted to answer either of these questions.)

Comparisons of hazards should always be made against the real alternatives, not against some hypothetical absolute standard (especially if the standard is the mythical "absolute safety"). For example, using a jet fighter's ejection seat is a dangerous act, with spinal injury not uncommon (ejection is a very violent process), but it is usually preferable to the alternative of riding a crippled aircraft down. On the other hand, if the aircraft is near the ground and upside down, it is safer to stay with the aircraft unless you have a very modern ejection seat. A realistic evaluation of the hazards of SDI must compare them against realistic alternatives, rather than just saying "they are too great". Much of the popular support for SDI comes from the perception that the alternative is a continuation of the current situation, which is perceived to be unacceptably dangerous. I don't think this an appropriate forum for discussion of the accuracy of these perceptions, but one should not forget that the alternative to risk often involves risks of its own.

Henry Spencer @ U of Toronto Zoology henry@zoo.toronto.edu

NASTRAN and the order-of-magnitude bug

David E. Bakken <bakken@hrsw2.UUCP>
19 Jul 88 21:23:43 GMT

I can't stand it anymore.

I was assigned the task of performing stress analysis on some roof bolts. I was supposed to do the NASTRAN run on the UNIX machine because it has some special math hardware, but I was in the middle of a game of rogue, so I used the IBM-PC on my desk. Unfortunately it was one of the really old ones, and it had the divide by 10 bug. As a result, my caculations were off, and I'm afraid a terrible thing happened. As a result, effective Friday, I'm leaving Boeing, to go work in a position where I can't hurt anybody. Monday I start my new position with Suzuki Motors Inc., in the suspension department.

Dave Bakken Ex-Boeing Commercial Airplanes (206) 277-2571

[Assessment of which planes NOT to fly deleted by your moderator. PGN]

"Person In The Loop" (Clifford Johnson)

Clifford Johnson <GA.CJJ@Forsythe.Stanford.EDU>
Tue, 26 Jul 88 13:43:05 PDT

> I completely agree with Will Martin and Bill Murray when
> they each insisted on adding to Zimmerman's piece a stronger
> statement about HUMAN fallibility.

I completely disagree. It's meaningless to construe the ignorance of a human to know an unknowable fact as a human "failure." Captain Will Rogers did not fail - he made his guess, as was required. Whether such a computer-ordered guess should ever be required is the the real issue, and if human fallibility is a factor, it lies in the stupidity of those who mandated this computer-driven gamble in advance of its execution.

> there WAS a man in the loop on the Vincennes -- the computers
> did not automatically fire the missiles without human
> intervention.

This seemingly logical statement is wrongheaded and very dangerous since it is a conception shared by congressional armed services committees and military alike. A Person-in-The-Loop (PTL) is as a matter of logic no more than a random number generator when, because of the shortness of time, computers provide essentially all of the information upon which an immediate "decision" is *required* from that person. In such a case, the real role that a person in the loop plays is to gamble whether an attack warning is real. To pretend that the human element means any more than this is the stuff of fairy-tales -- and whether a President, military commander, or computer operators make the guess is beside the point.

It is strictly incorrect to label such a response as NOT automatic. The response IS automatic. True, it is *randomized* by the human element, but it is certainly not made *discretionary* by the token interjection of a guess. The definition of "automatic" (in my Oxford American dictionary) is "working of itself without direct human control, done without thought, done from habit or routine." If time is insufficient for proper thought, it is improper to class a procedure as not automatic. True, routine participation of humans makes a response "not mechanized", but this is different from "not automatic". As General Ellis stated with regard to nuclear launch on warning drills, which are of the same computer-governed nature, "the purpose of that conference is to get a decision" - i.e. automatically, procedures force a guess in time to act.

Captain Will Rogers did no more than perform the function of adding an element of randomization to the Vincennes response, because he could not exercise proper judgment in that time frame. His response was inherently automatic. The gamble was not sanctified because it was made by a Captain. Rather, the Captain's role was debased by his being required to gamble.

> Congress's "man in the loop" mandate is an unthinking
> palliative, not worth much, and it shouldn't lull people into
> thinking the problem is fixed.

This portrayal is far too sangine. The so-called "PTL amendment" is positively nauseating -- it states that 100% mechanical lethality for Star Wars is A-OK as long as someone somewhere sometime switches it on. Herb Lin informed me that he lobbied to make a CINC responsible for switching on the auto-boost phase SDI defense -- and failed. The amendment is a dumb green-light to automation, masquerading as a restriction.

Person in the Loop

"David A. Honig" <honig@bonnie.ICS.UCI.EDU>
Tue, 26 Jul 88 17:01:09 -0700

Will Martin in RISKS 7.26 mentions how the popular media does not explain the risks of using computers and the costs and benefits of including humans in the control loop. Here is a (true) homey anecdote illustrating this principle that perhaps the press ought to be aware of:

I went to a supermarket and separated a soft drink from a package of them. When the UPC label is scanned, a price of $2.00 shows up. At one store, the checkout woman didn't believe me when I interrupted her and said that the price was wrong and sent someone to check; if I had bought a lot of groceries at the time I probably wouldn't have noticed. At another store, the checkout person did notice the unusual price (ie, sanity checking) and automatically corrected it --her vigilance was probably due to the fact that I again wasn't buying many items and she was in the express lane where the throughput is lower.

The important point is, the "human in the loop" issue is NOT esoteric or complex: the PROBLEM is that the popular press either does not understand this or will not communicate it to the mobs; thus, the layman continues to misunderstand and mystify computers.

And when an operator fails to interact with a computer correctly, no-one in the public wonders whether the computer programmer knew anything about man-machine interfacing and human factors engineering.

Another example: the term "computer virus" is a valid analogy but most laymen don't understand viruses enough to see the similarity. Why can't the press use "self-copying program" or some other informative term? (Because it makes less exciting headlines!)

Security vs. Cost of Breakin

"David A. Honig" <honig@bonnie.ICS.UCI.EDU>
Tue, 26 Jul 88 17:01:09 -0700

There is no such thing as absolute security; one tries to make a break-in as expensive as possible, more costly than the benefits of success. Relevant to recent RISKS issues, notice:

Encoding a bank-card PIN on the card magnetically IS secure for your average person and your average wallet thief. (Of course, a card reader is a pretty simple device; also, a thief could go to a bankcard-reading house (do they exist?), just like thieves go to pawn shops that sell stolen goods and car thieves go to junkyards that sell stolen parts. But that's a lot of effort for limited (eg, $300/day) returns, and besides, the owner will stop the card quickly yielding no return.)

Since NMR and CAT machines cost hundreds of thousands (and there are no small versions of them, and they are expensive to run) it doesn't

matter if they can detect winning lottery cards.

Hacking central office switches - too easy?

Skip Montanaro <steinmetz!vdsvax!montnaro@uunet.UU.NET>
27 Jul 88 16:57:32 GMT

John T. Powers wrote concerning the problems Pac Bell was having with crackers accessing their switches:

> A simple callback system (something I introduced at IBM about 10 years ago, and common now) would, if used correctly, make it *much* harder to gain unauthorized access to a CO switch. In addition, it would probably warn of interest by unauthorized persons. Today, much more sophisticated security systems are not only available but cheap.

The problem, as I understand it from the article that was posted in Risks, is that the Pac Bell repair people need to dial in from wherever problems exist, in order to set parameters, run tests, etc. Callback modems are only useful if the party wishing access always calls from the same (or at most a few) location(s). User A dials in, says "I'm user A", and hangs up. The callback modem then calls the phone number associated with user A. A Pac Bell repair person won't have a fixed location at which s/he can be called.

Skip Montanaro, GE Corporate Research & Development (montanaro@ge-crd.arpa)

Re: PIN on PNB calling card

Roy Smith <roy@phri>
26 Jul 88 14:10:46 GMT

In RISKS, Volume 7 : Issue 27, Mark Mandel <Mandel@BCO-MULTICS.ARPA> said:
> a credit card still provides a security barrier of sorts in the signature.

Don't be fooled into thinking that signatures are any kind of security barrier. I had my AmEx card stolen once (well, actually, I think I forget it on the table in a restaurant when I left, but that's another RISK). You would not believe the charges that came through (with AmEx you get back one of the copies of the charge slip so you can see exactly what is what). Some charges came through with signatures which don't resemble mine in the least. Some came through with no signature at all. One even came through with "signature on file" hand-printed on the signature line.

Roy Smith, System Administrator
Public Health Research Institute, NY NY

Re: IRS Illinois Experiment

Allan Pratt <atari!apratt@ames.arc.nasa.gov>

Tue, 26 Jul 88 12:06:23 pdt

> [Discussion of security issues in filling out tax forms online.]

Forgive me if I'm wrong, but I thought the whole problem with computer security was keeping unauthorized people out of sensitive information and places where they can do damage. On a computer where there IS NO WAY to get access like that, what's the problem?

Set up a front end which fills out forms from the remote users. Then dump a day's forms to magtape, carry the tape to the processing computer, and process it! The magtape is probably not necessary: any data channel will do. The point is to leave no "trapdoor to the OS" commands on the front end... There is no security door, just a blank wall!

The reason a system like UNIX is insecure, I thought, is that there are trusted users (esp. root) and non-trusted users, and ways for anybody to masquerade as a trusty by guessing the password or otherwise violating security AND GAINING PRIVILEGED ACCESS. If there is NO SUCH THING as privileged access, where can you go wrong?

The only hole I can see is using a bogus SSN to screw up somebody else's taxes, but you can do that no matter how you get into the system or how secure the actual access is. I could do that on paper, too, until they match the signatures. How much flak would come down on the poor slob before they figured that out?

If there is a fundamental flaw in my reasoning, please enlighten me.

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

[Let me suggest a few problems. Suppose it runs on a nonsecure system. You can now browse through the other returns stored on the system and not yet dumped to magtape. Or, you might install Trojan horses that record other people's data even after dumped to tape, or delete some of their income or claim phony deductions if you wanted to cause them grief. Or, you might change the program to accept State Disability deductions when the IRS had claimed they were nondeductible. Or, suppose the program was proprietary; you might purloin it and set up your own value-added-service. Also, see the comment in the previous note on eyeballing signatures. Top-of-the-head stuff, but you get the idea... PGN]

Search RISKS using swish-e

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 30

Friday 29 July 1988

Contents

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

NASTRAN and ship steel

"Lindsay F. Marshall" <Lindsay_Marshall%newcastle.ac.uk@NSS.Cs.Ucl.AC.UK>
Thu, 28 Jul 88 10:03:46 WET DST

Talking of NASTRAN reminds me of something that happened when I worked for a company involved in shipbuilding. The steel ordered for a ship that was almost completed turned out to be too thin so some extra reinforcerment was needed. In order to find the best places for this they ran the whole ship through NASTRAN. This job ran for 17 hours and filled several Gbytes of disc with temporary files. The machine crashed when there was no more available disc space. It turned out that the run involved 32000 degrees of freedom, but nobody had done the back of an envelope calculations to see if it was practical...

Lindsay

JANET: Lindsay_Marshall@uk.ac.newcastle
UUCP: ...!ukc!newcastle.ac.uk!Lindsay_Marshall

Is vibration a known A300 problem?

Eric Roskos <csed-1!csed-47!roskos@daitc.ARPA>
Thu, 28 Jul 88 13:13:34 EDT

> Pilots on France's domestic airline, Air Inter, began a new strike last
> night as part of a three-year campaign over Airbus safety.

Are there safety concerns other than fly-by-wire involving the Airbus? Or is this "three-year campaign" just about fly-by-wire? The above suggests there may be other safety issues; due to 3 experiences with A300s, I have suspected for several years that there might be some problem with resonance of the body to engine vibrations during takeoff. However, I have no evidence other than firsthand observation as a passenger on A300s to back this up.

Eric Roskos (csed-1!roskos)

Business Week article on computer security

Woody <<WWEAVER%DREW.BITNET@CUNYVM.CUNY.EDU<>
Fri, 29 Jul 88 16:21 EDT

The August 1, 1988 issue of BusinessWeek contained as cover article, "Is Your Computer Secure? Hackers, Viruses, and Other Threats". The article, pages 64-72, is reasonably well written, without inflammatory text, and has few errors or misleading statements. The article is in essence examining the risk to the public and private sectors of computer usage and loss; and covers employee attacks (Gene Burleson's assault on the Fort Worth security firm USPA & IRA Co., and arrest for "harmful access to a computer"), physical security in light of accident (the Hinsdale disaster), child 'phrackers' and Ma Bell, adult hackers (the Chaos Computer Club and the Deutsche Bundespost) viruses, and the like.

It's a glossy article, but is filled with interesting bits of data, such as US expenditures on computer systems over the last four years versus estimated sales of computer protection goods and services. They have photographs of Richard Brandow and the programmer who created the McMag virus, Pierre Zovile' (err -- if I ever meet them in a dark alley...) and so on. Its nice to see some responsible journalism coverage in a general purpose magazine. Or perhaps this is just a measure of how important the private sector rates computer security...

Computers can increase privacy, too!

"Robert Weiss" <weiss@umnstat.stat.umn.edu>

Thu, 28 Jul 88 20:26:10 CDT

I regularly get reports from my congressperson on his activities, and a comment in one of the articles grabbed my attention before I could toss the mailing:

> "Technology provides the students with privacy ..."

A different sentiment than we usually read about in RISKS. This is from an article on a computer-aided adult literacy teaching project in St. Paul. PC's placed in individual booths provide both privacy and flexibility. If I was 30 years old and unable to read at a 4th grade level, the privacy issue would be important to me.

This made me realize that while large computers and networks may in general be detrimental to privacy, there _are_ possibilities for computers to increase privacy.

Robert Weiss

> [But probably not if untrustworthy people have authorized access to the system or to the data, or if people without authorized access masquerade. The biggest problem with putting really sensitive data about an individual that might be of interest to someone else (for revenge, blackmail, curiosity, leaking, etc.) may be that the temptation level has escalated. PGN]

Viruses - a medical view

John Pettitt <jpp@slxsys.specialix.co.uk>
Wed Jul 27 19:00:35 1988

Taken without permission from the Independent (which seems to have gotten it from the British Medical Journal):

VIRUSES could invade hospitals throught their computer systems, so new software used by doctors is being quarantined before it is allowed contact with patients' data, Oliver Gillie writes.

The Royal Infirmary in Glasgow isolated a computer virus in its laboratory among software destined for the cardiac intensive care unit. The virus was found by a technician who destroyed it before it was able to multiply.

Dr Gavin Kenny, an anaesthetist at the Royal Infirmary, said the virus was not malignant, but "as soon as it was found, we made a complete sweep to look for others and now we do regular checks".

"A virus can wipe out the memory on an entire disk - that would cause a lot of trouble although it would not put patients' lives in danger," he added. "But some viruses are benign. There is one which just comes out on Tuesdays. It says it is Tuesday and then it goes away again."

[stuff about what a virus is and the christmas tree deleted - jpp]

Dr John Asbury, another Glasgow anaesthetist, says a virus got into an intensive care unit in the city where it corrupted data and caused files to be lost. Dr Asbury writes about computer virus disease in the latest issue of the British Medical Journal.

John Pettitt, Specialix, Giggs Hill Rd, Thames Ditton, Surrey, U.K., KT7 0TR
{backbone}!mcvax!ukc!pyrltd!slxsys!jpp jpp@slxsys.specialix.co.uk

---

Apple viruses

John Saponara <saponara@tcgould.tn.cornell.edu>
Fri, 29 Jul 88 13:06:44 EDT

From batcomputer!cornell!mailrus!uwmcsd1!ig!agate!ucbvax!pro-carolina.cts.COM!gregp Fri Jul 29 11:52:17 EDT 1988
Article 7320 of comp.sys.apple:
Path: batcomputer!cornell!mailrus!uwmcsd1!ig!agate!ucbvax!pro-carolina.cts.COM!gregp
>From: gregp@pro-carolina.cts.COM (Greg Prevost)
Newsgroups: comp.sys.apple
Subject: Virus Information
Date: 26 Jul 88 21:54:43 GMT
Reply-To: pnet01!pro-simasd!pro-carolina!gregp@nosc.mil
Organization: The Internet

Ok folks, in the past few days I have seen some major stuff going on. There are at least two different viruses running around. One is called Cyberaids and the other is made by some group called Festering Hate. Here is some of the info I have picked up on it in the last few days.

- = - = - = - = - = - =

50/50: Warning Apple users
Name: Practor Fime #13 @4
Date: Sat Jul 16 17:16:14 1988

CAUTION:

ZLink+, ZLink.PBH, ZLink are all viruses, if you run ZLink then you now are the happy parent to a rodent virus. It seem Zlink has some sort of virus that attaches to files and stuff. My friend has it on his HD and it creates some file entry in the ROOT directory that is hidden from every utility EXCEPT APW or ORCA. Every time you boot the prodos with the virus it will do and ON-LINE vol check (even if you specifiy the exact pathname) and install the virus on systems files such as, Mr Fixit, Basic.system,Copy II+ etc....

- = - = - = - = - = - =

(92 of 100)
Titled : <*** W A R N I N G ***>
Author : Dr. Logic/Bill of [None]

Stamped: July 13, 1988 at 12:07 AM

There is a file going around (currently on the Hard Drive) called Z.LINK.PLUS.
It is supposed to be a terminal program somewhat like ProTERM. It is a decent program but the main reason I posted this is when you boot it up, it GOES TO EVERY ON-LINE DRIVE AND MODIFIES >BASIC.SYSTEM

On IRS direct computer access

<denbeste@OAKLAND.BBN.COM>
Fri, 29 Jul 88 09:09:58 -0400

I think this is going to fail. High school students all over the state will spend their evenings making up social security numbers and entering phony returns. Perhaps one time in thirty or so they'll hit pay dirt (a real social security number!).

The only way to prevent this is to have the machine know the names of the people who own the SSN - and reject any return which isn't right.

Only, having done that, what happens if the legitimate owner of the SSN doesn't enter their own name is quite the same way it is held in the database?

Perhaps the right answer is for the computer to categorize the returns into one of two groups: "Those where the name was correct" and "those which a human being will check for validity".

Steven C. Den Beste, Bolt Beranek & Newman, Cambridge MA
denbeste@bbn.com(ARPA/CSNET/UUCP) harvard!bbn.com!denbeste(UUCP)

Re: doing away with privileged users

Alan Silverstein <ajs%hpfcajs@hplabs.HP.COM>
Thu, 28 Jul 88 18:31:41 mdt

In 7.29, Allan Pratt said:

> If there is NO SUCH THING as privileged access, where can you go wrong?

Alas, there is NO SUCH THING as "NO SUCH THING as privileged access".

Why? Because computers aren't as smart as people and as trustworthy as their administrators. Situations inevitably arise which require ad hoc human intervention -- by privileged users.

What if there were no distinction of "privilege"? If any user could handle the interventions? There'd also be precious little protection of users's data from other users. Even cooperating users need protection from each other's mistakes.

Alan Silverstein, Hewlett-Packard HP-UX DCE Lab, Fort Collins, Colorado

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 31

Monday 8 August 1988

Contents

- Software failures cost Britain $900M per year, study claims
  Jon Jacky
- Lightning strikes (twice)
  PGN
- Computer failure delays flights at Logan Airport
  PGN
- A320 & A300 safety, risks of so-called experts
  Michael Pilling
- RISKS of Electronic Cash-registers
  Robin Kirkham
- Computer terminals and dermatology
  richard welty
- Computer System Vulnerabilities
  Rodney Hoffman
- Disaster Exposition
  Cliff Stoll
- Info on RISKS (comp.risks)

Software failures cost Britain $900M per year, study claims

Jon Jacky <jon@june.cs.washington.edu>
Fri, 05 Aug 88 09:29:58 PDT

This article appeared quite a while ago in ELECTRONICS ENGINEERING TIMES (June 13, 1988, p. 19):

BRITAIN SCRUTINIZES SOFTWARE QUALITY by Roger Woolnough

...(Two) studies were commissioned last year from Price Waterhouse and Logica plc by the Department of Trade and Industry (DTI), the government department concerned with virtually the whole of British industry. The Price Waterhouse study sought to establish the costs and benefits of applying quality-management standards to software. The parallel study by Logica exmained the possibility of harmonizing the civil and military

quality management standards.

The failure costs are expensive. For British industry, the report estimates them conservatively at $900 million a year, and that includes only software produced domestically and sold on the open market. If imported and in-house software were included, the failure costs would be much higher. And on top of that there are substantial indirect costs, which Price-Waterhouse could not quantify.

Price Waterhouse estimated that implementing a quality system would mean additional costs for a typical supplier with 50 to 100 employees of between $360,000 and $450,000 a year. Initial setup costs could be between $180,000 and $270,000, with no difference between large and small companies.

The study was unable to estimate the reduction in failure costs that would result from wider use of quality systems but did work out the savings required to justify them - a 10 to 15 percent reduction in total failure costs over the life of a system.

"If we consider costs and benefits to suppliers only," says the report, "a reduction in failure costs of 35 to 40 percent would be required to sustain the investment in a quality system. ... An improvement of this size is possible, but far from certain. Therefore it is possible that software suppliers could incur net costs as a result of introduction of a quality system. The evidence suggests that most users are not prepared to pay higher prices for software simply because a quality system was used by the supplier."

(The Logica study compared various standards for software quality assurance, namely NATO's AQAP documents, used by the British Ministry of Defence, and international ISO9001. Logica found little difference in substance and recommended standardizing on ISO9001).

- Jonathan Jacky, University of Washington

Lightning strikes (twice)

Peter G. Neumann <NEUMANN@csl.sri.com>
Mon 8 Aug 88 14:33:09-PDT

On 31 July 1988 lightning struck the drawbridge between Vineyard Haven and Oak Bluffs on Martha's Vineyard MA, paralyzing the three-phase controls and then ricocheting into the elevated transformer. As a result the Lagoon Pond access for 40 sailboats and tall powerboats was sealed off for almost three days. (This was the same weekend that the ferry Islander ripped a hole in its belly when it ran aground, backlogging 500 cars. And your moderator was there, finally getting a little vacation so that you all could get a little vacation from RISKS.) The previous lightning strike, only three weeks before, had closed the bridge for 24 hours. [Source: Martha's Vineyard Times, 4 August 1988, p. 1.]

Computer failure delays flights at Logan Airport in Boston

Peter G. Neumann <NEUMANN@csl.sri.com>
Mon 8 Aug 88 14:40:33-PDT

On 5 August 1988, air traffic was delayed because a new software tape designed to relay departure information to air traffic controllers sent data to the wrong controllers. It took an hour to replace the software. The delays at Logan lasted for about 6 hours, tapering off slowly from one-hour delays. Delays also propagated to nearby airports. [Source: Boston Globe, 6 August 1988]

A320 & A300 safety, risks of so-called experts

Dr Chocberry)
Thu, 4 Aug 88 15:39:47 EST

This is from an article in the "Australian" 2-Aug-88 retyped and abbreviated without permission:

> Two pilots blamed for air crash
>
> Following an official report to the French transport minister last week, responsibility for the crash of an Airbus A320 into trees at an airshow in eastern France has been blamed on pilot Michel Asseline & co-pilot Pierre Mazieres. The A320 gets a clean bill of health.
> Cockpit talk recordings from the black box revealed startling over-confidence on the part of both men. Mr Asseline told Mr Mazieres on the ground he would not use the aircraft's sophisticated alpha-floor computer system, which automatically boosts the fuel supply to the engines when its speed, altitude and incline indicate a danger of stalling.
> He also disconnected a secondary system to boost power so he would have maximum manual control, boasting that he would fly the aircraft at 30m at low speed, with just enough power to keep the plane at maximum incline without losing height.
> Mr Asseline would then put on full throttle to climb away at a steep angle, he said.
> "You want to show off, huh?", the co-pilot said.
> Several times before the critical manoeuvre the crew contemptuously dismissed visual and aural wornings emitted by the onboard computers.
> The pilot responded to one by saying: "Knock that one off, it's getting on my nerves."
> Just before the fly past the co-pilot said:" `Right, you're coming down to 100 feet, do it, do it."
> "Right, I'm going for it, disconnect the fuel boost system."
> "Watch out for the pylons ahead, eh? You've seen them, yeah?"
> "Yeah, yeah, don't worry."
> The co-pilot then told the pilot to put on full throttle. As the aircraft failed to gain height the pilot was heard to curse.
> Neither pilot has been formally accused of causing the crash,

although the transport ministry said a judicial investigation could still bring charges.

Soon after the crash I saw an american TV report on the crash which featured a so called "COMPUTER EXPERT" (the caption on the screen, no mention of his field or qualification was made) stating that "if it's pilot error it must be systems failure", without knowing anything of the architecture of the software. Obviously there is a risk in trusting experts in a field you know nothing of, because you (in this case the NEWS service) are inclined to believe them.

Eric Roskos (Risks 7.30) asks, is vibration a common problem in A300's. I have often experienced the throbbing you refer to, and have noticed that the wings virtually beat on take off. I think this intended or at least seen as an acceptable side effect of the wing geometry during take off. In general, I suspect aircraft maintenance in the US is taken far less seriously than here and this may be partly to blame.

Michael Pilling (bigm@banana.cs.uq.oz)

RISKS of Electronic Cash-registers

<munnari!mimir.dmt.oz.au!rjk@magni>
08 Aug 88 15:37:14 EST (Mon)

Years ago when cash-registers could only add, it was safe. Nowadays they can subtract as well, and so cash-register operators can't, and so you lose your change. It's been happening to me more and more often over the past couple of years. I explain:

Formerly, the cash-register would add up all the prices of the things you bought, and at the end the operator would hit the `Total' button, and the till would pop open. You would proffer your money, and your change would be made up by counting out coins, then notes, adding to the total price and working up to the tendered value. Then you got the docket.

But now, at the end of the sale, the operator punches in your tendered amount, and the cash register calculates the change, which is then counted out into your hand in the reverse order -- big notes first, then little ones, then the coins get balanced delicately on top.

Then you get the docket shoved at you. The coins slide off the notes in you hand, fall and roll under the checkout counter. Gone forever. Can't give you any more change, till won't balance. Your own mistake. Get out of the way, your holding up the other customers.

Australia has recently been inflicted with a $2 coin, and the old $2 note has benn withdrawn. The Treasury, in its infinite wisdom, made the coin smaller than most of the other coins and out of an exceptionally light aluminium alloy, which made the problem even worse.

I once asked a checkout girl why they had reversed the order of counting out

the change. She said they were told to do it that way, since they "made less mistakes" and it was "easier". Actually, I expect the reason was so that the supermarket could sweep under the counters and collect all the dropped change.

Robin Kirkham CSIRO/DMT rjk@mimir.dmt.oz (My opinions, only)

Computer terminals and dermatology

richard welty <steinmetz!welty@uunet.UU.NET>
Fri, 5 Aug 88 17:19:22 edt

The following short article recently appeared in Cutis, a journal of dermatology (I don't know the exact issue.) A note indicates that the authors are with the Department of Dermatology, University of Maryland School of Medicine. Reprints are available from:

Dr. Burnett
Division of Dermatology
University of Maryland Hospital
22 South Greene Street
Baltimore Maryland 21201

This article is reprinted without permission.
Figure 1 (omitted) is merely a picture of a user and an IBM PC.

``Dermatologic Manifestations in Users of Video Display Terminals''

Marline L. Cormier-Parry, MD
Gary V. Karakashian, MD
Joseph W. Burnett, MD

It is not surprising that with new technological advances, new dermatologic entities also appear. Rosacea is a cutaneous reaction pattern thought to be provoked by many factors including foods, alcohol, heat, and cold. Recent reports have implicated exposure to video display terminals (VDT) as another causative factor (Figure 1). Since the first reports from northern Europe in 1982, when VDT exposure was related to the excerbation of rosacea, acne, seborrheic dermatitis, and poikiloderma of Civatte, more recent reports have appeared (references 1-3).

The symptoms and dermatitis associated with VDT use are usually paresthesia or pruritus of the upper cheeks or perioral area with either solitary papules or a fine erythematous papular eruption. The typical features of most cases of VDT-associated dermatitis were onset of the eruptions two to three hours after daily use of the VDT, improvement of the dermatitis on days the unit was not used, and, low ambient relativie humidity at the time of the exposure.

VDTs produce several types of electromagnetic radiation. The cathode ray tube emits low-energy x-rays. The phosphor material of the screen emits ultraviolet, visible, and infrared radiation. The electronic circuits produce radiofrequency and very-low-frequency radiation. Most electrical

and electronic equipment can generate ``electrical noise,'' a low-level, broad-spectrum electromagnetic radiation. To date, no adverse biological effects in humans have been documented from these electromagnetic fields and the level of radiation emitted is far below the occupational standards set by federal authorities (references 2-4).

The electrostatic fields, however, are more likely to be the causitive agent of VDT dermatitis. Electronic fields are noted around most VDTs at low humidity and tend to disappear at higher humidity (reference 5). Most cases of VDT dermatitis have occured in northern Europe and during the winter months, when the relative humidity is less than 40 percent. Further evidence for this hypothesis comes from obserrvations that when the electrostatic fields were reduced, operators' dermatitis and other symptoms were also reduced. Whether this is a direct effect of the field itself or an irritant dermatitis from airborne particles is unknown. Several female operators have reported the deposition of their makeup on the VDT screens at the end of a working day. However, the deposition of volatile and particulate air pollution on the skin can be induced by electrostatic field charge (reference 2). Furthermore, there have been several reports of patients who were able to prevent the dermatitis by the use of physical blocking agents, such as titanium dioxide or Duoderm.

Recently, computer manufacturers have introduced VDTs that have no static electric fields as a means of preventing dermatitis. Electrostatic shields are also available and widely used in northern Europe. The shield, which is placed in front of the VDT screen, becomes conductive at relatively low humidity and thus eliminates the static field. Improvement with these shields, however, is usually temporary since their conductivity diminishes with time. In the United States, the use of a skin-colored ``sun-block'' cream containing 2 percent titanium dioxide with iron oxides was recommended. It showed some success in preventing VDT symptoms and the associated dermatitis (reference 4). Improvement in some Norwegian cases was noted after the substitution of antistatic floor carpeting in the work area (reference 3).

References

1. Liden C, Wahlberg JE: Work iwth video display terminals among office employees. _Scand J Work Environ Health_ 11: 489-493, 1985.

2. Berg M, Liden S: Skin problems in video display terminal users. _J Am Acad Dermatol_ 17: 682-684, 1987.

3. Nilsen A: Facial rash in visual display unit operators. _Contact Dermatitis_ 8: 25-28, 1982.

4. Fisher A: ``Terminal'' dermatitis due to computers (video display units). Cutis 38: 153-154, 1986.

5. Berg M, Langlet I: Defective video displays, shields, and skin problems. _Lancet_ 1(4): 800, 1987.

--

richard welty 518-387-6346 GE R&D, K1-5C39, Niskayuna, New York
welty@ge-crd.ARPA {uunet,philabs,rochester}!steinmetz!welty

Computer System Vulnerabilities

Rodney Hoffman <Hoffman.es@Xerox.COM>
2 Aug 88 08:43:51 PDT (Tuesday)

RISKS Moderator Peter Neumann has an op-ed piece in the August 2 Los Angeles Times with the headline

A GLITCH IN OUR COMPUTER THINKING
We Create Powerful Systems With Pervasive Vulnerabilities.

Although they are overly-familiar topics to RISKS readers, I trust the moderator will permit a few quotes:

> Our civilization seems to have developed an inherent craving for easy answers, especially regarding technology. In particular, we tend to anthropomorphize computers and endow them with human intelligence -- while at the same time we deify them and endow them with infallibility....
>
> One of the most serious problems in computer-related systems is the inadequate protection of such valuable resources against unintended or malevolent misbehavior by authorized as well as unauthorized computer users -- and against malfunctions of the computer systems....
>
> [Brief mentions of computer-related problems at Pacific Bell, NASA, banks, the Vincennes, false arrests....]
>
> Computers and their communications are frequently vulnerable, but they are also limited by the intelligence and wisdom of their developers, administrators and users.
>
> It is a common myth that the complexity of such systems deters malfeasants. In fact, the attackers may understand the system better than many of the defenders. Digital technology is inherently finite -- there are only certain possible cases. The number may be large, but often there are shortcuts that eliminate the need to search exhaustively for a needed clue -- password, design flaw or code bug....
>
> There are no guaranteed complete solutions that can prevent computer-system malfunctions, intrusions and both accidental and malevolent misuse. But there are prudent measures that can be taken to reduce the risks. [Better design and implementation, better laws, ...] Above all, we must have a computer-literate populace -- better educated, better motivated and more socially conscious.
>
> Computer security vulnerabilities are pervasive, but they are not usually evident to the general public. Depending on flawed computer systems will lead only to bigger disasters. Overall, we must work much harder to understand and openly consider the true risks of using computers.

Disaster Exposition

Cliff Stoll <cliff@Csa4.LBL.Gov>
Wed, 3 Aug 88 21:59:02 PDT

Hi Riskees!

Last month's Computer Assurance conference -- COMPASS '88 was a gas -- really good talks on electronic voting systems, computer assisted automotive problems, fly-by-wire risks, and averting computer domino effects. Our illustrious hero, Peter Neumann, gave a couple outstanding talks. For those of you who haven't met him, he's just as quick with puns behind the podium as when moderating our forum.

COMPASS dealt with averting disasters. On the flip side is the
1988 International Disaster Congress, Nov 9-11, in Chicago.
Sounds weird to me:
"How was your meeting?" "Complete disaster."

It sounds neat, but I can't afford $675 admission,
so if any of you Riskee's are going, could you post your notes to Risks?

Keynote Speaker:
Edward Teller (inventor of the H Bomb, promoter of Star Wars)
"Gaining a Global Perspective of Disaster Control"

Some session titles:
Prior Planning for "Acts of God"
Foreseeing Deliberate Acts of Violence
Anticipation of Technology's Catastrophes
Identifying Beforehand the Impact of Epidemics
Success Stories of Disaster Preparedness
Implemented Programs for Minimizing Natural Disaster Impact
Preventive Approaches to Controlling Deliberate Violence
Ventures for Mitigating Technological Accidents
Restraining Threats of Mass Disease
Sustaining Corporate Morale in Midst of Nature's Attack
Allocating Resources while under Siege
Damage Control at Accident Scenes
Minimizing the Spread of Current Epidemics
Cleanup Following Natural Disaster
Recovery from Violence Induced Calamity
Post Exposure Measures for Restoring Health
Timely Action following International Incidents
Eliminating All Effects of Sustained Disaster
Replacing Resources Destroyed by Natural Catastrophe
Restoring Order from Chaos of Deliberate Violence
Total Recuperation from Epidemic
Recovery Through Repossession and Reparations

Speakers are from:

Bay Area Earthquake Preparedness Project,
Univ. Rome, Univ. Delaware
Emergency Preparedness Council of Canada
Int'l Assoc of Fire Chiefs
Cincinnati Hazardous Materials Task Force
Maryland Institute for Emergency Medical Services
Disaster Services for American Red Cross
National Governor's Association
California National Guard
Association of American Railroads
Armed Forces Institute of Pathology
Israeli National Police
Association of Contingency Planners, American Savings/Loan
Federal Insurance Administration

Also, there'll be a Disaster Exposition, "A showing of products for
anticipating, coping with, and recovering from disaster."
Yikes -- what do you think they sell to recover from
one of Teller's thermonuclear bombs?

Registration/Details:
Kotch & Poliak, 708 3rd Ave, NYC, 10017 212 557 6950

Cheers, Cliff Stoll Cliff@lbl.gov

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 32

Tuesday 9 July 1988

Contents

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

Privacy in computer age (no place to hide)

Sayed Banawan <banawan@sun1.cs.uh.edu>
Wed, 3 Aug 88 11:26:44 CDT

From Houston Chronicle (August 2,1988) without any permission:

No Place To Hide Your Privacy In Computer Age
by Albert E. Denny (Denny is a free-lance writer in Baltimore. MD)

IN case you haven't noticed, your privacy is being invaded and eroded at an unprecedented pace nowadays, thanks to advances in communications technology growing out of proliferation of computers. No matter who are you or where you live, information concerning your personal life and lives of family members is being pumped into databases at a scary rate.

Even your own computer may be watching you. The congressional Office of Technology Assessment reported that computers are being used to keep tabs on as many as 6 million workers, from government employees to bank tellers. In some cases, employers monitor the productivity by programming the machines to record how many keystrokes users make per hour.

Computerized phone systems track how many calls workers make or operators handle. They can also be rigged to listen in on conversations. "It's Big

Brother at its worst." says U.S Rep. Don Edwards, D-Calif. "Just because you get a job doesn't mean you lose your constitutional rights."

No clear legal definition of privacy exists, but experts agree on a few basics: It means the right to keep personal affairs to yourself and to know how information about you is being used. The issue has big implications on information companies.

"I think the industry feels that individuals must sacrifice a certain amount of privacy in the information age," says Peter A. Marx, an attorney specialized in computer law. The public disagrees. A 1984 Harris Poll found 75 percent or respondents "very" or "somewhat" concerned about threats to privacy.

There is no place to hide. If you are a living, breathing person moving about in society. making purchases and paying bills, a growing file of information exists on your personal life and habits that is little short of mind-boggling. Such information is compiled in diverse ways.

If I buy a toaster made by a major appliance company, what right does it have to include with warranty (to be filled by me) a battery of questions relating to my age, sex, occupation, hobbies, marital status, etc.? The obvious reason such information is is being compiled is so it can be fed into a computer and the resulting data used for misleading (and unauthorized) purposes such as the sale of mailing lists to specialized companies for money.

When I buy common stock or subscribe to a financial publication, the subsequent barrage of solicitations from financially related companies interested in selling me a product or service can only be traced to the sale of such confidential information to those seeking to profit from it. That is a gross misuse to privileged information and I resent ti.

We are all at the mercy of computers which spew out massive amounts of information on individuals that can be collected, cross-matched and manipulated to generate much more detailed profiles of U.S. citizens than ever before - sometimes in a matter of seconds. This information can affect everything from credit ratings to welfare eligibility to your chances of renting an apartment or landing a job.

consider the following major sources of data that feed into computers, giving the most intimate details of your personal life:

The Internal Revenue Service exchanges data with state and local tax authorities to check the accuracy of tax returns.

Your Social Security number, the code that third parties need to tap into computerized information on you, is available to at least 125 government and private agencies.

About 40 states sell direct-mail companies the information you provide when registering a vehicle or applying for a license. That reveals you age, sex, Social Security number - even, through deduction, your income range.

The FBI's National Crime Information Center has more than 10 million centrally stored recoreds of criminal histories - all available to state and local authorities.

The five largest credit reporting companies control records on more than 150 million individuals.

Some states are computerizing their court documents, making it easier to

monitor everything from eviction to criminal proceedings.
Most banks are allowed by law to give out information on customers' accounts and credit histories to state government investigators.
Life insurance companies, by tapping a central data base run by a company called the Medical Information Bureau, can find out details about your medical history from claims information provided by insurers.
Direct-mail companies, hungry fro your business, comb through some of the above records and other information, churning out lists of specific individuals whom salesmen or political campaign may want to contact.

Get used to those increasingly more personal letters and the chummy phone calls from salespeople who want to sell you something. They know everything about you, and the best defense may be to sign up for a course in sales resistance.

Follow-up to legal hypothetical (RISKS-6.42)

<CEREUBEN%AMHERST.BITNET@MITVMA.MIT.EDU>
Mon, 8 Aug 88 08:26 EDT

In March of this year I posted a hypothetical in RISKS Digest, volume 6 issue 42, concerning the proper allocation of rights in software between programmers and their employers. At the time, I was writing a law school paper on this issue, and was curious to see how well the legal standards I was uncovering lined up with your perceptions of the basic equities. Here is the promised follow-up on that posting.

I. THUMBNAIL LEGAL ANALYSIS OF THE HYPOTHETICAL **

** What follows is not practical legal advice, but merely a brief theoretical analysis.

Briefly, The hypothetical dealt with a programmer named John Allan, who is hired to design and implement a touch-sensitive help utility for use in his employer Medicomp's medical database, MEDSTORE. Allan later uses this same utility in the development of a tax expert system, TAXELF, and is sued by his former employer Medicomp. The posting asked for your thoughts on the extent to which Medicomp, by contract or law, should be able to limit Allan's later use of code and ideas developed during his employment with them.

The current law's treatment of such a situation is at best complex and at worst completely unsettled. Principles of copyright, patent, trade secret, unfair competition and contract law all potentially apply. In each of these areas, there are relatively few statutes and written judicial opinions which deal directly with computer software. New cases are constantly being brought; however, most of these are settled out of court.

Therefore, I can't possibly provide you with a definitive "answer" to the John Allan problem. What follows is merely the OPINION of a recent law school graduate as to how this particular hypothetical MIGHT be approached by a court today. Bear in mind that the law is in a state of flux. Also note that I have NOT yet been admitted to the bar, and that in any event, this should NOT be

taken as practical legal advice.

As many of you correctly noted, Allan would most likely be covered by a carefully drafted employment ageement, assigning to Medicomp the ownership of any copyright or patent in the original program. Even if the contract did not speak to ownership issues (which would be unusual these days), Medicomp would probably by seen by a court as owning the copyright. The program was written by "an employee" and "within the scope of his employment," and would therefore qualify as a "work for hire" under the Federal Copyright Act.

As owner of the copyright, Medicomp could prevent Allan from using the actual code in his tax system, both through direct copying or rewriting from memory. While de minimus copying of insignificant or nonunique modules would probably be allowed, Allan's wholesale appropriation of the entire help utility would likely be seen as a copyright violation.

Less settled is the extent to which Allan could use the non-code elements of the program. A number of courts would extend Medicomp's copyright protection to the program's structure and organization. Few, however, would bar Allan from the use of touch sensitive help in general.

The important thing to note is that, for the purposes of copyright law, Allan's status as creator does not give him any greater right to use the software than members of the general public.

As an ex-employee, however, Allan is bound by a duty not to use or disclose the "trade secrets" or "confidential information" of his employer. This duty is inferred at common law, but would likely be specifically stated in Allan's employment contract as well. The precise definition of "trade secret" and "confidential information" varies greatly from state to state. Moreover, as Medicomp would likely be seeking equitable relief, i.e., to enjoin Allan from further use of the software, the court would be free to engage in a more open-ended balancing of the equities than would be permissible if purely monetary relief were sought.

Given the flexible nature of current trade secret doctrine, a court could really go either way on this issue. The touch sensitive utility at issue here does seem to fall within the generally accepted range of protected information: Allan's solution to implementing touch sensitive help would probably be considered sufficiently "novel" by a court, the utility was likely "held out as secret" by Medicomp, and the product has obvious commercial "value." On the other hand, a court would also consider the extent to which the program was developed prior to employment, the fact that the TAXELF and MEDSTORE do not compete, and, in a minority of jurisdictions, the extent to which Medicomp contributed in the development process apart from salary.

More generally, though the court may undertake the analysis from a number of different angles (trade secret, copyright, contract, etc.) the following general factors would likely emerge as relevant:

1) The nature of the employment relationship and the language of the employment agreement.
2) Protection of employee's interests in intellectual property predating the employment relationship, and in job mobility

3) Protection of employer incentives to invest
4) The nature of what was taken - intangible ideas vs. tangible code. Unfortunately, this arguably reduces to the question of whether Allan can change the code enough to make the second utility seem like an independent creation.

II. SURVEY RESULTS

I received close to 200 responses from programmers, employers, students and professors involved in various aspects of computer technology. Unfortunately, despite my specific instructions to the contrary, many of the responses seemed to be an account of what the writer felt the law was, rather than how she would like it to be. Therefore, it would be misleading to draw any conclusions along the lines of "90% of those surveyed thought Allan should not be able to reuse specific code."

However, I can draw some general conclusions. The responses seemed to line up surprisingly well with the treatment under the current law as summarized above. Again, it is not clear whether this is an indication that the law tracks what is considered reasonable in the industry, or that RISKS readers are well-informed of their legal rights. The responses also reflected the highly controversial nature of the allocation question and the range of issues considered relevant. Issues discussed included:

1) The importance of information-sharing to program development. Many of the responses mentioned that programmers are most efficient in an environment where information is freely shared. None of the cases or statutes I read seemed to even contemplate the importance of information-sharing in the development of an appropriate software protection scheme.

2) The importance of protecting the employer's investment through ownership rights. There was almost universal agreement that the employer investor should own the software. The responses differed, however, on how broadly ownership rights should be defined.

3) An employee's right to her general programming skill. There was, however, substantial disagreement as to exactly what constitutes "general skill". There was general agreement that it does not include actual code, but the responses diverged greatly as to whether general skill includes code written from memory, program structure and functionality.

4) The importance of competitive harm. Lack of competitive harm was often seen as a factor in favor of allowing a departing employee to make use of software owned by his employer.

5) The nature of the software in question. A few of the responses suggested that some kinds of programs should be

singled out as being more worthy of protection than others. (For example, an employer arguably should not be able to sue an employee who recycles a standard sort program.)

6) The affect of pre-employment assignment agreements on inventive behavior. While most people seemed to feel such agreements are valid and enforceable, many noted that incentives to invent, and in particular, to reveal those inventions to one's employer, would be greatly reduced.

7) Problems in policing ownership rights in software. Many of the responses noted the difficulties inherent in proving misappropriation, particularly where the defendant originally wrote the code.

8) The team-programming problem. Some of the responses opted for employer ownership simply because it would be next to impossible to determine which employees were primarily responsible for the develpment of a product, and impractical to give ownership rights to low-level programmers only marginally involved.

9) Software Tools. A minority of the responses suggested that denying an employee access to actual code she wrote for a prior employer could greatly undermine her effectiveness and marketability.

Thank you all for your responses. They were a great help to me in analyzing and critiquing the current law's allocation scheme.

Again, I'm not in a position to give practical advice, but I would like to say this much: the law in this area is extremely muddled. There are no clear cut answers, and the few emerging standards are subject to change. So, don't take anything for granted. Also, after reading hundreds of cases, statutes, articles, etc., I am convinced that there is a GREAT need for more input from the technical community. Many judges, laywers, legislators and commentators, even those of us with some background in computer science, do not have a firm grasp of all the intricacies and unique needs of the software develpment industry. If the law is to serve its function of promoting the development and accessibility of software products, the legal and technical community must work hand in hand.

Preliminary A320 Inquiry Results

martin@bashful <@RELAY.CS.NET:martin@bashful>
Mon, 8 Aug 88 20:01:59 PDT

Aviation Week and Space Technology, August 8, 1988 has a paraphrase of the preliminary report; if you want more details than my paraphrase of a paraphrase contains, I refer you there (I'm too lazy to type in any substantial extract).

The major points of interest to RISKS readers would seem to be:

* The CFM56 engines and the engine controls responded properly to control inputs; the throttles were advanced 5 seconds before impact, and the engines had spooled up to 83% N1 speed by impact. This was not enough to produce any useful change in aircraft attitude or speed (indeed, the aircraft's airspeed would seem to have continued to decrease during this time).

* The pilot and copilot (apparently informally) planned to fly at 100 ft. AGL for the flyby, with no planned airspeed (oops). They ignored three radar altimeter callouts below this altitude (the radar altimeter gave six callouts in the 25 seconds between 100 ft. and impact, three after the throttles were advanced).

* The pilot intentionally disabled the alpha floor protection mode in the autothrust system; this mode is intended to provide protection against windshear accidents. Alpha floor refers to the symbol used for angle of attack--alpha floor would normally apply takeoff/go-around thrust if the angle of attack were to exceed 15 degrees. As you can see from following the altitude/speed profile of this flight, large aircraft don't accelerate and climb very well (that is to say, at all) at low speeds and high angles of attack. It takes a long time to spool up large high-bypass engines, and it takes even longer before that energy input has any effect on the aircraft.

At any rate, Aviation Week says the investigation is now trying to determine why the pilot and copilot were unaware of their situation (that is, why they were apparently unaware that they were lower than they intended, and presumably why they were unaware that they were in deep trouble with energy (= airspeed) management: airspeed dropped from 151 kt. at 25 seconds before impact to 112 kt. one second before impact).

In unrelated French (un)safety news, SNCF is investigating two changes to brakes on its trains, following the second major accident in Paris: they are considering replacing the conventional vent-all-the-air-and-eeeeeek emergency brakes with an intercom to the driver, and they are considering removing the disconnect valves which enable train crews to disable the brakes on an individual carriage. (The source for this fine item is New Scientist; the British railway-isms may give that away.)

--Martin Harriman
martin@cadev4.sc.intel.com

Computer terminals and dermatology (Re: RISKS-7.31)

Steve Philipson <steve@aurora.arc.nasa.gov>
Mon, 8 Aug 88 21:18:54 PDT

I found the article posted by steinmetz!welty@uunet.UU.NET (richard welty) on "Computer terminals and dermatology" very interesting. There were several statements in the article that directly contradict several studies I've read. For example:

VDTs produce several types of electromagnetic radiation. The cathode ray tube emits low-energy x-rays. The phosphor material of the screen emits ultraviolet, visible, and infrared radiation. The electronic circuits produce radiofrequency and very-low-frequency radiation. Most electrical and electronic equipment can generate ``electrical noise,'' a low-level, broad-spectrum electromagnetic radiation. To date, no adverse biological effects in humans have been documented from these electromagnetic fields and the level of radiation emitted is far below the occupational standards set by federal authorities (references 2-4).

Current design VDT's (within the last 10 years) emit essentially no detectable x-rays. Light, from the u/v through i/r range, is of low intensity, less than from typical office incandescent and flourescent bulbs. RF intensities are generally lower than the ambient intensities from local radio and TV stations. The article does point out that no known adverse effects have been linked to these sources at these levels, so the earlier statements aren't really significant.

The article notes onset of dermatitis during conditions of "low ambient relative humidity at the time of the exposure", and that "The electro-static fields, however, are more likely to be the causitive agent of VDT dermatitis." These observations are consistent, as low humidity increases the tendency of electrostatic devices to precipitate out charged airborne particles. However, causality is not observed: " Whether this is a direct effect of the field itself or an irritant dermatitis from airborne particles is unknown."

About three or four years ago, a panel at the ACM SIGCHI conference discused the issue of VDT hazards to health. Dermatitis was observed in several case studies. It was discovered that the effected operators had the habit of touching the screen and later touching their faces. This action served to transfer particulates that had precipitated out of the air from the screen onto the faces of the operators. The industrial "fix" to the problem was to institute a procedure of cleaning the screens of all VDT's at the beginning and end of each work shift.

Blocking agents would be expected to help as they would not only reduce skin contact with the precipitated material, but also reduce the incidence of operators touching the screen, as this action would coat the screen with blocking agents transferred by the fingers.

The conclusion of the SIGCHI panel was that the greatest danger to VDT users was through poorly designed workstations that contribute to poor posture, increased back and muscle strain, and visual problems causing eye strain, headaches, and even seizures.

Straighten up out there, and clean those screens regularly!

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 33

Wednesday 9 July 1988

Contents

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

Cascaded Inference and the Vincennes affair

<CFEEHRER@G.BBN.COM>
2 Aug 1988 20:28-EDT

I have become interested in the dialog lately re: Vincennes and the question of thresholds for declaring radar blips hostile (see, for example, Wellman, 9 July; Johnson, 10 July; Estell, 12 July) and would enjoy some comments in regard to the following proposition: "There's nothing wrong, in principle, with "binary thinking/decision making" if ALL of the information available for a choice among competing hypothesis is employed in the computation of posterior odds." What may have gone wrong in the Vincennes case is that not all of the information that was available came to be used. Most notably, perhaps, the diagnostic value associated with target aspect ratio, which the press tells us was more-or-less head-on and at short range relative to the design envelope of Aegis, did not enter into the decision in a formal way. It is interesting to

me that difficulties with interpreting an image formed under such circumstances was one of the first explanatory notes to surface during coverage of the encounter. Thereon hangs the story below.

I'm suggesting that, however, accurate the Aegis sensor and signal processing systems may be, the information presented to the human decisionmaker is apparently equivocal ("unreliable") at certain combinations of range and aspect and provides the basis for a very complex judgment even when a good estimate of the priors can be made. It seems to me that the situation, corresponds closely to what has been called "cascaded inference" in behavioral decision theory. In prescriptive approaches to decision making in this kind of situation, there are two sets of conditional probabilities: the probability of a datum conditional upon an hypothesis, and the probability of a REPORT (verbally, electronically or otherwise delivered) conditional jointly upon an hypothesis and a datum. If the components of these are known or can be estimated, then the probability of a report conditional upon an hypothesis can be easily calculated. In effect, the decision maker is required first to adjust the nominal diagnosticity of the report to reflect the reliability of the source -- "interpretability of the image" is a better term here -- and then to apply this adjusted datum to the hypotheses under evaluation using Bayes' rule. In the scenario I'm conjuring, the first task would have been to make a (cognitive) adjustment of the diagnosticity of the displayed image (i) given the hypotheses, "(a)ttack", "(n)o attack", and then to compute the posterior odds (p(a:i)/p(n:i) given p(i:a) and p(i:n). (Note that at optimal ranges/aspects, the diagnosticity would be assumed to be nearly perfect, while at non-optimal ranges/aspects, it would be considerably less than perfect -- a little circular but OK for now! The point is that, while the electronics remain the same, the intrinsic value of the image, its utility, for purposes of deciding between two (or more) mutually exclusive hypotheses varies.)

When one compares the posterior odds achieved with an adjusted datum with those achieved with an unadjusted datum, the results can be startlingly different! (This is not a good forum for lengthy equations, so I'll simply ask you to believe that assertion! I'd be happy to send along some references and a short demonstration to anybody who's interested. For a quick perspective, consider that a likelihood ratio of 9:1 falls to approximately 4.3:1 when one reduces the reliability of the reporting system from 1.0 to 0.9. That can lead to quite a different decision with the same set of priors.)

Research in decision making in medical, military command, process control/QC, and trouble-shooting contexts regularly demonstrates two phenomena: (1) Decision makers are typically not trained to make decisions "by the numbers", even when that is possible -- it's not a skill that comes naturally; (2) The few decision makers who are familiar with quantitative decision aids have rarely been taught means for coping with unreliable data. The sad thing is that virtually ALL data, whether delivered through eyes and ears or complex sensor systems are unreliable from time to time and/or for certain purposes. So, is it surprising that, in situations characterized by high stakes and great stress, wrong hypothesis are occasionally supported and correct ones discarded?! (There is an interesting literature associated with attempts to create descriptive models of what decision makers actually do which suggests that optimal procedures for discounting equivocal information are rarely intuited, but that they can be trained. References on request.)

The "story" above is clearly a house of cards -- plausible maybe but unverifiable at best. Who knows if ANY quantitative reasoning went on at all -- but I do want to suggest that binary decision frameworks may not be as limiting as they may seem at first if they are properly implemented. I'm a strong supporter of neural net/fuzzy set approaches, but only if simpler algorithms are found wanting and their alternatives are not. cef

---

"Virus" Bill

"Joseph M. Beckman" <Beckman@DOCKMASTER.ARPA>
Fri, 5 Aug 88 10:36 EDT

"Computer Virus Eradication Act of 1988"

(a) Whoever knowingly --

(1) inserts into a program for a computer information or commands, knowing or having reason to believe that such information or commands will cause loss to users of a computer on which such program is run or to those who rely on information processed on such computer; and

(2) provides such program to others in circumstances in which those others do not know of the insertion or its effects;

or attempts to do so, shall, if any of such conduct affects interstate or foreign commerce, be fined under this title or imprisoned not more than 10 years, or both.

Entered July 14th 1988 by Mr. Herger (congressman from CA) for himself and Mr. Carr; referred to Committee on the Judiciary, to amend title 18.

Joseph [You can lead a Trojan horse to Waterloo, but you can't make his legislator think. PGN]

More RISKy ATM's

Dave Horsfall <munnari!stcns3.stc.oz.au!dave@uunet.UU.NET>
Thu, 4 Aug 88 14:39:34 est

From Neville Angove's column in "Computerworld", 29th July:

``According to a number of sources in the systems programmer community, the recent media noise concerning ATM fraud/failures indicates a number of severe problems being faced by financial institutions with ATM networks. As the size and usage of these networks have increased, so have the security risks, due to the fact that the knowledge of ATM characteristics and network limitations have become more widespread. The most serious rumour is that one bank has evidence that someone has discovered a means to decode the PIN encrypted on to the magnetic strip

of stolen ATM and credit cards. [It is not generally well-known that in Australia at least, that strip encodes your PIN!]

Another factor causing concern, especially to the more knowledgable members of the public, is the increasing use of lower-cost -- and probably lower-quality as a result -- ATMs by the smaller banks which want to provide a competitive service but cannot justify the cost of higher-quality equipment. A model of the ATM favoured by one bank is so lacking in "intelligence" that it can only run in on-host mode [?], and circumvents the problems of storing transaction details by printing them as they occur on to a paper cash register roll (an ironic solution, since the manufacturer originally made its name as the giant of the cash register business). [Well, perhaps they need to use up a warehouse full of rolls!]

The increasing number of instances in which ATM networks have not functioned as claimed, or where stolen cards have been used to milk the victim's account in apparently impossible circumstances, is evidence enough of some fundamental design faults or deficiencies in a number of -- but not necessarily all -- ATM networks. Public claims by the banks that their networks are secure do not agree with concerns they have expressed privately, but it is unlikely that the community will see any improvement until the problems with ATM networks are brought to light through the legal system.''

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

Keeping Autos and Drivers in Suspense

"Joseph M. Beckman" <Beckman@DOCKMASTER.ARPA>
Tue, 9 Aug 88 10:25 EDT

From "The History and Future of Automobile Suspension" by Rick Castelli in CORRIDOR TODAY July 29 1988 p9 (No copyright or reprint directions on page)

"As a result of Japanese competition, all of the major American and German automakers are racing to provide their own versions of 'smart' suspensions as soon as possible...Both Lotus and Volvo's systems have eliminated the use of springs, shocks, and antiroll bars, as well as other components. Instead, hydraulic cylinder devices are incorporated that detect various lateral and vertical wheel motions. Sensors are also used to detect other factors and forces upon the car. All of this data is fed into a computer which subsequently inputs instructions to the hydraulic cylinder devices to adjust wheel deflection and angle. What results is that the wheels never leave contact with the road, and the body of the car automatically leans precisely into turns, thus maintaining a stable flatness, even through emergency maneuvers. This is a phenomenal advantage! In a sense, it makes the car feel as if it's floating independently above the road.

Likewise, this could be one disadvantage -- among others. Drivers will lose that inner sense of knowing when a car is at its limits of handling, and might get too confident for their own welfare."

The last point reminds me of some study done years ago. Some researcher, S. Peltzman, found that the mandatory use of seat belts would not save (net) lives. The reason given was that drivers feel 'invincible' (or more so) when wearing them. Consequently, they became less attentive to driving, increasing the number of accidents. Although they did a good job of protecting the driver, many accidents killed pedestrians; more than the number of drivers and passengers they saved. Joseph

Airbus Cockpit Alarms

Fred Baube <fbaube@note.nsf.gov>
Tue, 09 Aug 88 13:24:58 -0400

munnari!banana.cs.uq.oz.au!bigm@uunet.UU.NET
(Michael Pilling (Dr Chocberry)):

> Several times before the critical manoeuvre the crew
> contemptuously dismissed visual and aural wornings emitted by the
> onboard computers.
> The pilot responded to one by saying: "Knock that one off,
> it's getting on my nerves."

Pardon my naivete, but ..

This sounds like the Amtrak crash. Any irritating+persistent alarm that "cries wolf" gets defeated with whatever tools are at hand. If the condition causing the alarm is an everyday event (Amtrak), or an event that was out of the ordinary but nonetheless intended (e.g. fancy airshow maneuver), and the same alarm is to be used for a REAL problem, then the alarm won't be there when it's needed.

Don't these guys that design alarms consider a "cry wolf" factor? Would they want to be trying to fly an airliner with an unnecessary racket disturbing their concentration ?

A-320 investigation

Steve Philipson <steve@aurora.arc.nasa.gov>
Tue, 9 Aug 88 12:26:56 PDT

Re: martin@bashful <@RELAY.CS.NET:martin@bashful> posting on "Preliminary A320 Inquiry Results".

>* The pilot and copilot (apparently informally) planned to fly at 100 ft.
> AGL for the flyby, with no planned airspeed (oops). They ignored
> three radar altimeter callouts below this altitude (the radar altimeter
> gave six callouts in the 25 seconds between 100 ft. and impact, three
> after the throttles were advanced).

The warnings would have been expected, and the crew would have planned to ignore them. The whole point of this maneuver was a low altitude fly-by. Ground proximity warning systems would call the altitude, so there would be no reason to be alerted to a "problem" that was part of the intended flight path.

>* The pilot intentionally disabled the alpha floor protection mode in the
> autothrust system; this mode is intended to provide protection against
> windshear accidents. ...

This also seems reasonable for the flight path desired. Manual control of engines and AOA was desired, so again, this intentional disabling of automatic systems seems reasonable.

> ... large aircraft
> don't accelerate and climb very well (that is to say, at all) at low
> speeds and high angles of attack. It takes a long time to spool up
> large high-bypass engines, and it takes even longer before that energy
> input has any effect on the aircraft.

This is not quite true. Jetliners attain close to maximum climb performance at high angles of attack, but with maximum thrust. The recommended windshear escape maneuver is to raise the nose to just below stall AOA and hold maximum power. The problem IS in spool-up time of the engines. What I'm most interested in is how two highly experienced pilots allowed RPM to decrease below reasonable values for this type of maneuver.

One of the first things you learn when flying jets is that you must keep RPM up if you will need a rapid application of power. Did the engine control system retard power below the intended setting? Did the combination of enabled and disabled systems cause the engine settings to go below what the pilots had intended?

The investigations into why the crew was unaware of their situation is critical to assesments of the safety of the A-320. The unusual manuever and crew selected configuration may have had much to do with the cause of this accident. We know that conditions not accounted for in the design of complex systems are often the root of system failure. Many of us are very concerned about digital control systems for just this reason. We will not know if this crash was really "pilot error" until those elements of this accident are thoroughly explored.

Federal charges brought against accused teen-age hacker

Mike Linnig <linnig@skacsl.csc.ti.com>
Tue, 9 Aug 88 22:28:52 CDT

CHICAGO (AP) -- A teen-age high school dropout is charged with using his personal computer to break into AT&T and government computers and steal more than $1 million worth of software.

"This is not malicious mischief," U.S. Attorney Anton Valukas said in announcing the federal charges Monday. "It's a felony."

Herbert Zinn Jr., 18, also is accused of advertising on a computer bulletin board how to electronically break into AT&T's computers.

The charges against Zinn mark the start of "an aggressive position toward computer crimes," Valukas said.

Zinn allegedly committed the crimes when he was a juvenile, and could be sent to prison until his 21st birthday in August 1991.

Federal agents raided Zinn's home last year and confiscated three computers and software allegedly stolen during the electronic break-ins.

The telephone at Zinn's North Side residence went unanswered this morning.

Zinn was quoted in today's editions of the Chicago Sun-Times as saying that since the raid on his home, he had not pursued his computer techniques "with quite the same vim and vigor."

He said he nonetheless hoped eventually to resume his schooling and become an electonics engineer, the newspaper said. Zinn would not discuss details of the case, it said.

The federal charges were brought after Zinn had been arrested several times, including for alleged computer break-ins at the Keller Graduate School of Management and at Commodity Perspective Inc., both in Chicago.

"Before and after the computer break-ins (at Keller and Commodity Perspective), Zinn was, by his own admission, breaking into AT&T computers," Valukas said.

Court documents said Zinn broke into an AT&T computer at the North Atlantic Treaty Organization's Maintenance and Supply Headquarters in Burlington, N.C., and an AT&T computer at Robins Air Force Base, Ga.

Valukas said the software taken from NATO and the Air Force base were "low level in terms of sensitivity."

Agents raided Zinn's home after an AT&T security officer logged onto the so-called Phreak Class-2600 computer bulletin board and spotted messages signed by "Shadow Hawk," a code name the goverment said the teen-ager used.

In the messages, Shadow Hawk bragged that he had gained access to AT&T computer files. In a similar message, Shadow Hawk made the mistake of including his telephone number, which the security officer spotted, the government said.

The purpose of the Texas-based Phreak Class-2600 is "to educate computer enthusiasts . . . to penetrate industrial and government sector computer systems," said William J. Cook, an assistant U.S. attorney.

The government said Zinn also tried to electonically break into computers at the Washington Post's accounts payable department, a hospital in South Bend, Ind.; and computers in Columbus, Ohio; Rye, N.Y. and Pipe Creek, Texas.

Orbit 100,000 self-guided "brilliant" weapons, Reagan advised

Jon Jacky <jon@june.cs.washington.edu>
Wed, 10 Aug 88 08:53:39 PDT

The following story appeared in THE SEATTLE TIMES, Aug 9 1988, p. A3:

SDI OFFICIALS URGE 'PEBBLES' OVER 'ROCKS' by Dan Stober, Knight-Ridder News

A dozen high-ranking "Star Wars" officials met privately with President Reagan two weeks ago to gain his backing for a new weapons idea: swarms of five-pound

rockets, known as "brilliant pebbles," that would orbit Earth and decide on their own to attack Soviet missiles.

The rockets, once launched, would not require a command from the ground to attack.

"It's effectively a shield over the planet, consisting of these things, and if anything pierces the shield that doesn't come from an allowed launch point ... it gets knocked off," said Bruce McWilliams, who headed a lab team that developed the optical sensors for "brilliant pebbles."

It would take 100,000 such rockets to defend against the next generation of Soviet missiles, a Livermore study concluded.

...(the idea) was advanced by the Lawrence Livermore National Laboratory... the classified White House briefing was given by Livermore physicist Lowell Wood, a protege of the controverial Edward Teller.

- Jonathan Jacky, University of Washington

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 34

Friday 12 August 1988

Contents

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

"Eye focusing found to be VDT hazard."

Denis Haskin <denis%wellesley.edu@RELAY.CS.NET>
Wed, 10 Aug 88 18:03:29 edt

From the Boston Globe, Wednesday, Aug 10, 1988

BERKELEY, Calif. - Regular work in front of a VDT screen may cause a premature loss in the eye's ability to focus, according to preliminary research by a University of California optometrist. A deterioration in eye focusing among people in their 20s and 30s was the No. 1 problem found in 153 patients treated at the university's Video Display Terminal Eye Clinic, said researcher James Sheedy. The study, prepared for a symposium in Ohio, was the first clinical report of eye-focusing problems in VDT users.

They may be right. I've been working with display screens for about the last five years, and lately (last three years) usually most of a working day. Until recently I had no need of glasses but on my last exam the doctor recommended some; they aren't very strong, but I have noticed a difference. My eyes are much less tired after a full day at a terminal now.

Denis W. Haskin, Technical Analyst, Digital Review, Boston, MA

Privacy (Again) (Re: RISKS-7.32)

<willis@rand-unix.ARPA>
Wed, 10 Aug 88 15:23:36 PDT

Denny's article is a rehash of old points and old concerns but updated with a few contemporary examples. He fails to raise and comment on a central point.

He asks (to paraphrase the point) what right a manufacturer has to ask all manner of personal questions on the warranty form. He should note (but did not) that he nor anyone else is under no obligation to answer all manner of questions in such a situation. The warranty in no way will be affected if he declines to answer.

My best bottom line on personal privacy is this:

1. Information intrusion and its consequences is just another one of those risks of living in this world.

2. Each of us better be well informed of when we are legally obligated to answer questions and give personal information, and when we are not.

3. Each of us will have to understand that like other risks of living in our world, privacy will require us to take care of ourselves, using whatever mechanisms society and/or governments have provided and whatever innovations we can indvidually create.

4. To the extent that people behave like information-sheep and mindlessly answer every question put before them by any inquiring agent, then privacy will be eroded more and more and self-protection will become all the more difficult.

Trying saying NO when asked for personal information; you'll be surprised at how often it won't make any difference.

Willis H. Ware

"Virus" Bill (RISKS-7.33)

Jerome H. Saltzer <Saltzer@ATHENA.MIT.EDU>
Thu, 11 Aug 88 00:27:31 EDT

> (a) Whoever knowingly --
> (1) inserts into a program for a computer information or commands,...
> (2) provides such program to others in circumstances in which ...

Wonderfully put. As I read that language, installing Sun NFS 3.0 in your favorite operating system and then running it at your site would be a felony. Perhaps this bill is not such a bad idea as it seems at first.

(Not to pick on Sun . . . there are dozens of other good examples. Installing your vendor's newest system release without alerting all your users would probably become a felony, too.)

Jerry

Re: "Virus" Bill

<denbeste@OAKLAND.BBN.COM>
Thu, 11 Aug 88 12:06:50 -0400

It has been long known among law enforcement experts that severity of punishment is less of a deterrent than certainty of punishment.

If a given crime has the death penalty, but only one change in a thousand of being caught, convicted and punished, then there is no deterrence. If the penalty is light but the chance of punishment is high, there is deterrence. (Which is why no-one throws rocks through the windows of the Police station or paints graffitti on its wall.)

So it is with this bill. The penalty is as stiff as the constitution allows, but the chance of being caught is vanishingly small. The only virus-authors I have heard have been identified were boasting about it. If they'd kept their mouths shut, they wouldn't have been found.

But just finding them, hard as it is, is the easy part. How do you prove that they are the author? JURY-prove, I mean.

Even without this bill, there were potential penalties. A large corporation who was hurt by a virus could have sued the virus author, if they knew who it was and could prove it. But the search usually would have cost more than the damages.

What this bill DOES do is give the FBI grounds for a serious search for virus authors. But what if the author is overseas? The current most common virus for the Amiga was written in Switzerland.

Steven C. Den Beste, Bolt Beranek & Newman, Cambridge MA
denbeste@bbn.com(ARPA/CSNET/UUCP) harvard!bbn.com!denbeste(UUCP)

RE: "Virus" bill

<kovner%vsg1.DEC@decwrl.dec.com>
Fri, 12 Aug 88 10:27:52 PDT

While I doubt the entire anti-virus bill was published in Risks Digest 7.33, the following excerpt seems to have problems:

> (a) Whoever knowingly --
> (1) inserts into a program for a computer information or commands,
> knowing or having reason to believe that such information or commands will
> cause loss to users of a computer on which such program is run or to those who
> rely on information processed on such computer; and

This sounds like it makes the DELETE (or rm) commands illegal! Even more, what would it mean for operations people who have (and supply) command files to clean up disk areas? (e.g. PURGE on VMS or deleting *.tmp) UNIX(r) systems should have NOCLOBBER always set, and remove the >! construct. Gear up disk drive production if this takes effect.

I hope there is something in the bill which excludes commands necessary to the normal functioning of the system, and those which allow the user to lose things himself. This should be written to cover only those "information of commands" which are surreptitiously inserted, or exist in programs which are not expected to erase data.

Steve Kovner, Digital Equipment Corporation

(The opinions expressed above do not necessarily represent the opinions of my employer.)

A Visit To the Clinic

<ssc-vax!ssc-bee!ellisb@beaver.cs.washington.edu>
Wed, 10 Aug 88 09:45:24 pdt

I went to a local medical clinic yesterday for the first time. After a few minutes I wondered if I had come to the right place. The first clue that something was wrong was the complaint of the couple in front of me in line at the front desk. They had received a bill in the mail for over 1,000 which was surprising to them since they had prepaid provider insurance. (Prepaid provider insurance allows the doctors office to bill the insurance company without the patient having to submit insurance claims). Furthermore their account number for insurance was also scrambled and didn't match the credit card that is usually provided with prepaid insurance. The receptionist explained that the computer had been broken and that they should ignore the bill since they should not have gotten it in the first place.

When I went up to the desk upstairs someone was having to pay cash because "the computer is messed up and cannot bill your insurance directly". Of course I was depending on *my* prepaid provider plan to pay and had maybe 5 dollars to my name so I was a little concerned. I had also noticed that there were several assistants stashed in corners hand sorting what appeared to be bills.

After the doctor found out I worked with computers he told me what had

happened. The clinic had recently replaced their computer system with a new one and disposed of the old one. The new computer took the current balance * number of patients in family and produced bills for all the patients that had been in the clinic including people with prepaid provider type of insurance. A nurse who had worked at the clinic received a bill for over 4,000 dollars. Apparently it had taken her bill of approximately 80 dollars and multiplied it by both her immediate family, and her grandchildren. I hope they keep their medical information on a separate computer! Take 3000 aspirins and call me in the morning :-)

It seems to me that using the new system that the clinic or the installer should have performed some kind of check before they converted over to the new system or at least run the two systems in parallel until they verified the operation of the new system. At least I would attempt to verify the new system before I mailed out bills to hundreds of angry customers. I guess I will have to wait till the end of the month and see how my bill comes back but since there is only one of me at least they should be able to calculate it correctly. At least my back is feeling better. It does make me a little angry that "the computer is always to blame" when it appears that the real fault lies with the humans that install, program, and feed the computer.

I think I understand now why we test software and look at the results. I have seen more than one instance where the end user of a computer product trusted the computer so much that they stopped checking the results even when the were obviously wrong. Maybe we need to educate end users to not put blind faith in the computer and as software producers to test our software and make it as idiot proof as possible. Even a simple spot check of some of the bills at the clinic could have prevented an expensive and embarrassing mistake.

Brian Ellis, Boeing Aerospace,Seattle, WA 98124-2499 (206) 773-2599
My boss has both opinions and humor but the views expressed here are mine.

Aegis beaten by binoculars? (Trusting computers and/or people?)

Martyn Thomas <mcvax!praxis!mct@uunet.UU.NET>
Thu, 11 Aug 88 10:11:55 BST

The following letter appears in Flight International, 6 August 1988. Copied without consent.

"When I was a kid I was intrigued by an advertisement for a pair of binoculars with which I would be able to see 'the craters of the moon' and 'France as if it was only a mile away'. I saved up and bought them, and when they arrived they were, in fact, a rather nice pair of wide-angle 10*50s. I never saw France, but I certainly saw the craters on the moon.

The other day, from a vantage point on the South Downs, I thought I'd put the old 10*50s to the test again. Visibility was okay, but there was a lot of wind and fairly low cloud around. I looked in the general direction of Gatwick Airport and after only a minute I saw the unmistakable profile of a One-Eleven climbing out, smoking visibly. Then a slightly larger aircraft - almost certainly a 737, a -200 I'd say, the engines were not big enough to

be a -300. These are some binoculars, I thought: even if France doesn't look a mile away, at least Reigate Hill does.

Only a few minutes passed before a relatively huge shape climbed into the air - an ex-BCal DC-10, the overall design of the livery clearly to be seen. Not only was this a DC-10, and not a TriStar, but it was an ex-BCal '10. It turned north soon after take-off, and flew away from home a while, and even from this aspect it was definitely a '10. I watched it climb and turn, disappearing into cloud and then reappearing again. Good sport this, I thought, give me a clear day and I could follow a widebody all the way from, er ... well ... Bandar Abbas?

Just a moment! What's going on? Am I really distiguishing between near-identical wide-body aircraft from all aspects at almost *three times* the slant range at which the captain of the USS Vincennes launched two Standard missiles and destroyed an A300?

In disbelief I double-checked the scale of the map in the AA Book of the Road. No doubt about it, these aircraft are well over 20 miles away, and that '10 must have been 30 miles out when I lost sight of him. The Airbus was only nine miles out, at 7500 feet on a clear day when the missiles were fired. Okay, the A300 was motoring, but tell me which direction he was coming from and with my 10*50s I reckon I'd have narrowed the field to a 757, 767 or an A300 before you could say 'F-14' - and certainly before he got within nine miles.

I've never seen an RCA Aegis system advertised in Exchange and Mart but, even if I do, I don't think I'll buy one.

[signed]
ANDY COUPLAND, 20 Holmcroft, Crawley, Surrey, RH10, 6TW "

Airbus

George Michaelson <munnari!ditmela.oz.au!G.Michaelson@uunet.UU.NET>
Fri, 12 Aug 88 11:25:31 +1000

Old news is no news but reflective journalism improves with age.

The developments in the airbus crash mirror the situation of the late 19th C when warning devices began to be installed in Railway Engine cabs & signal boxes. Getting highly trained "elites" to accept a machine warning is hard. If they can switch it off, many of them will, until they crash themselves into extinction. Does history ALWAYS repeats itself?

For me, the key point is NOT to let this stand as a reason to take a human out of the system. The system worked, the pilot failed, but PLEASE leave them in there.

Aegis, is almost but not quite an opposite situation. Both the System AND its users failed. Some [me?] would argue aegis 'failed by design' since attempting to 'predict' with <100% accuracy something you cannot really 'see'

is not the same thing as 'identifying' with <high-enough> accuracy something you might need to destroy. The failure was inevitable.

Congressman Smith seems to show that the process of procurement for the DoD is sufficiently flawed as to make ANY complex system inherently doubtful.

George Michaelson, CSIRO Division of Information Technology

ACSnet: G.Michaelson@ditmela.oz Phone: +61 3 347 8644
Postal: CSIRO, 55 Barry St, Carlton, Vic 3053 Oz Fax: +61 3 347 8987

SDI rationalizations

Steve Summit <scs%adam.pika.mit.edu@RELAY.CS.NET>
Tue, 2 Aug 88 22:23:47 EDT

There's an article in the August Issue of Reader's Digest by Tom Clancy (author of The Hunt for Red October), entitled "Common Sense About Strategic Defense." Given RD's editorial stance, I was surprised to see this title until reading the article revealed that "Common Sense" entails that SDI is an appropriate, nay, desirable response to Mutual Assured Destruction (MAD). Most of the article is fairly predictable, relying on things like blind acceptance of the SDI "research" "results" reported so far, but the paragraph on software really made me laugh (or cry):

> Some opponents have questioned whether we could program computers with the millions of calculations necessary to fight a battle against ICBMs. I don't doubt we can. In the 12 years since supercomputers were introduced, these devices have moved from doing millions of calculations per second to billions, and are now about to exceed ten billion calculations per second. Those who believe our computing capabilities are not up to the challenge ignore the fact that a computer that once filled a building would now fit on their wrists. These people just haven't been paying attention.

Steve Summit, scs@adam.pika.mit.edu

Re: Misidentification of persons as criminal by computers

99700000 <haynes@ucscc.UCSC.EDU>
Wed, 10 Aug 88 22:03:04 PDT

We have had discussions of cases in which computer data bases wrongly identified innocent people as criminals. I just read an interesting counter-case, in a Bob Greene column in an Esquire magazine from a few months ago.

Briefly, a man killed his live-in fiance, disposed of her body, and then reported her as missing and mounted an effort to find her so as to establish an

alibi for himself. A police officer on the case suspected the man, for some reason, and tried to look him up in a computer database, presumably NCIC. He got nothing, so he tried variant spellings of the man's name and turned up the identity of a fugitive from justice with almost the same social security number and birth date as his suspect. Confronted with this, the man confessed to being the fugitive and waived extradition to be tried for the earlier crime. With further grilling he confessed to the murder.

Greene also noted that while the Chicago police were looking for the missing woman, her unidentifiable body was found in Indiana where the murderer had taken it. But there was no communication between the two police agencies in this matter instance.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 35

Monday 15 August 1988

Contents

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

Re: Privacy (difficulty of witholding "private" information)

Jon Jacky <jon@june.cs.washington.edu>
Mon, 15 Aug 88 09:15:05 PDT

> (In RISKS 7(34) Willis H. Ware recommends (in response to a posting
> about nosy questions on warranty cards): (people are) under no obligation
> to answer all manner of questions in such a situation - (try) saying NO
> when asked for personal information...

This is good advice. However, the implication of this posting, that individuals can significantly control information about their activities that is collected by firms they do business with, is not true in general.

Information about you that firms learn in the course of doing business with you is their property, not yours. It has significant commercial value

which some firms exploit aggressively. Much of the commercial value derives from the ability to process this information by computer. Some of the firms that do this are utilities, so you do not have the choice of "saying NO."

For example, the local telephone operating company in the Seattle area has offered a service in which it makes its directory listing information available to other marketing firms in machine readable form. Salespeople have always been able to work through the telephone book of course, but the value that the computer adds is that the listings can be processed in various ways. Most obviously, the marketer can ask for just the phone numbers in a given set of zip codes to focus on particular neighborhoods. Having the data in machine readable form makes it easy to match against other databases the marketer may have. Note that this is a product that the phone company sells, just like it sells local telephone service.
There was a bill introduced into the Washington State legislature that would have prohibited utilities from reselling information about any customer without that customer's written permission. It was killed in committee due to lobbying efforts by utilities.

> (Willis Ware says) Information intrusion and its consequences is just
> another one of those risks of living in this world.

I believe this takes a much too passive view of the situation. Information about individuals (the real stuff of which privacy is an abstraction), like many other commodities of value, is being struggled over by different parties that have competing and somewhat incompatible interests. Who eventually ends up with what will result from a combination of laws, regulations, legal proceedings, and market activity. The exact contents of these remain to be seen, but participants who take a passive view of this struggle are likely to wind up with very little.

- Jon Jacky, University of Washington

[By the way, the Sunday New York Times of 31 July had a nice article by John Markoff on this general subject, including mention of the American Express practice of selling off selective mailing lists (e.g., rich tennis players who frequent resort hotels). PGN]

Re: Keeping Autos and Drivers in Suspense

<treese@ATHENA.MIT.EDU>
Sat, 13 Aug 88 18:56:28 EDT

In RISKS 7.33, Joseph Beckman describes Sam Peltzman's studies on seatbelt usage leading to no net decrease in auto accident fatalities. It is worth noting that Peltzman's studies were highly controversial and the methodology was somewhat questionable. Later studies did not show the same results. Unfortunately, I do not have any references available now, but there was a time when I researched the literature on this quite extensively.

The bottom line is still that wearing seatbelts is a good idea.

Win Treese, Digital Equipment Corporation/MIT Project Athena
Affiliation given for identification purposes only.

[Aggressive drivers who feel safer because they are belted up are more likely to be hazardous. The computer analog relates to overly endowing your system -- the results are more likely to be hazardous. PGN]

Re: Cascaded inference (in RISKS-7.33)

g.l.sicherman <ihnp4!odyssey!gls>
13 Aug 88 22:18:31 GMT

In Risks Digest 7.33, cfeehrer@BBN writes:
>
> ... What may have gone wrong in the Vincennes case is that not all of the
> information that was available came to be used. Most notably, perhaps,
> the diagnostic value associated with target aspect ratio, which the
> press tells us was more-or-less head-on and at short range relative to
> the design envelope of Aegis, did not enter into the decision in a
> formal way. ...

Cfeehrer goes on to discuss the use of a-priori probabilities and Bayes's rule, and describes how "cascaded inference" can go badly wrong. I agree completely, and would like to extend the discussion.

For many years the A.I. research community has been divided over which is more important in an intelligent system: a big knowledge base or clever inference methods. In the field, a majority of researchers seem to prefer clever inference methods, mainly because knowledge is hard to come by and harder to encode.

Meanwhile, the probability and statistics research community is divided into Bayesians and non-Bayesians. (There are other important philosophical controversies in probability and statistics, but I won't go into them here.) In brief, the Bayesians hold that to get useful probabilities by calculation, you must calculate them from known a-priori probabilities. The non-Bayesians hold that you can get useful probabilites even without knowing enough a-priori probabilities to let you apply Bayes's rule. The non-Bayesians accept Bayes's rule--and seek to augment it.

A non-Bayesian theory prominent in A.I. research is that of A. P. Dempster, as formalized by his student G. Shafer. This theory seems to be popular because (1) its formulas can be computed routinely, and (2) being non-Bayesian, it can dispense with some a-priori probabilities that Bayesians would regard as necessary. Whether the Dempster-Shafer theory is a valuable contribution to probability theory or a worthless and misleading exercise is yet to be established. It falls in roughly the same grey area as Fuzzy Set Theory.

I'm a Bayesian myself; I have little to add to Boole's remarks on

this subject in his _Laws of Thought._ I'm not too worried about "certainty factors" and similar oddities in the world of probabilistic computation. But I shudder at the risks of using military systems that ignore some of the fundamental a-priori probabilities in the field! When such systems take appropriate action, it can only be considered a fortunate accident.

Col. G. L. Sicherman

Re: "Eye focusing found to be VDT hazard."

Brint Cooper <abc@BRL.MIL>
Fri, 12 Aug 88 19:53:07 EDT

Denis Haskin quotes the Boston Globe, "A deterioration in eye focusing among people in their 20s and 30s was the No. 1 problem found in 153 patients treated at the university's Video Display Terminal Eye Clinic..."

Then, he reports his own experience, "I've been working with display screens for about the last five years,...on my last exam the doctor recommended (glasses and) I have noticed a difference."

I suggest that this sort of thing proves nothing. All my life, I have known people who read a great deal in their childhood and wound up with extreme nearsightedness. I knew a chap who repaired small timepieces most of his life and, in his 60's was nearly blind. No one suggested that books and precision repair are risky to one's vision. Perhaps any intensive visual activity, unbroken over long periods of time, can lead to vision problems. I suggest that multiply blind, retrospective and comparitive studies of all these risk phenomena are long overdue.

"Risks of using computers must be assessed against the risks of not using computers." _Brint

Eye Focusing and VDTs

"Anthony G. Atkielski, Honeywell Bull Inc." <Atkielski@HIS-PHOENIX-MULTICS.ARPA>
Fri, 12 Aug 88 19:46 MST

I've been working with VDTs since 1980, and I'm now 27 years old. Long ago I noticed that my right eye didn't focus very well on distant objects. The way that eye behaved (trying to focus, overcorrecting, etc.) made me suspect that the constant close-up work with the VDT was reducing the ability of my eye to accommodate for distant vision. The problem goes away after a couple days away from the CRT, and no similar problem has manifested in the left eye. My ophthalmologist tested my eyes and found nothing wrong (!); he said there was no evidence to indicate that using VDTs over long periods permanently affects vision.

It's interesting to see a news item that mentions exactly the problem I've noticed, among people in my age group. If there really is a link between VDTs

and some focusing problems, what can I do about it? I still have to use a VDT every business day (I'm using one to compose this message). I'm not going to get glasses because I have the distinct feeling that the problem would eventually disappear if I could just stay away from a VDT long enough. What are my options? Didn't anyone notice problems like this in the days before VDTs? After all, VDT users aren't the first people to engage themselves in close-up work for long periods.

Anthony Atkielski, Honeywell Bull Inc.

Myopia (near-sightedness) and VDT use

Jeremy Grodberg <jgro@pnet06.cts.com>
13 Aug 88 22:30:28 GMT

Are there any studies about extensive VDT use leading to Myopia? I had 20/20 vision when I started working as a programmer, and it has steadily gotten worse since. Further more, when I take a long absence from working (several weeks), my eysight seems not to change, but when I return to work, it seems to get worse rapidly. Maybe its my imagination, but I have no evidence that wht I thinks is happening isn't.

Jeremy Grodberg

Can current CAD/simulation methods handle long-term fatigue analysis?

John R. Galloway <jrg@apple.com>
Wed, 10 Aug 88 17:24:48 PDT

As more and more of the design of (an aircraft say) is done on a computer, less and less of the design will be handled by "rule of thumb" type decisions. While this seems a good thing, I wonder if there is a down side concerning aspects of the design that were implicitly included in the old rule of thumb or handbook days (from years of experience) and are not necessarily included in the computer model. The case I am thinking of is the airliner a few months ago where the top of the fuselage riped off (en route from one of the Hawaiian Islands to another). Are current supercomputer simulation methods capable of handling the complexity of long-term stess, fatigue, corrosive environments, etc., all of which were (apparently) factors in the Aloha incident? Also I am not at all sure that such things were handled any better before wide-spread use of CAD -- I am just asking the question. Any aeronautical engineers out there?

ATMs and PIN protection: twice silly victims in Boulder

"Gary McClelland" <MCCLELLAND_G%CUBLDR@VAXF.COLORADO.EDU>
Fri, 12 Aug 88 15:45 MDT

The latest ATM scam from Boulder: The campus newspaper reports that a thief has been lifting bank cards from unattended backpacks in libraries on campus. A day or two later, the victim receives a call from a "bank security officer"

saying that a suspect has been caught trying to use victim's stolen bank card to extract cash from an ATM. As part of collecting "police report" information, the "bank security officer" asks victim for the PIN so that he can complete the investigation. Victim gives the PIN over the phone and then "bank security officer" uses the stolen card and the PIN to extract maximum allowable cash limit.

Is this why it is good to have a human link in computer security systems?

Gary McClelland, U. of Colorado

[For those of you whose response is, "What, another silly story like this one?", the point is that scams like this succeed with amazing frequency. We've had quite a few. PGN]

Re: Orbit 100,000 self-guided "brilliant" weapons, Reagan advised

Amos Shapir <nsc!taux01!taux02.UUCP!amos@Sun.COM>
11 Aug 88 11:06:07 GMT

[in RISKS-7.33, contributed by Jon Jacky]

>"It's effectively a shield over the planet, consisting of these things, and
>if anything pierces the shield that doesn't come from an allowed launch
>point... it gets knocked off," said Bruce McWilliams, who headed a lab team
>that developed the optical sensors for "brilliant pebbles."

How on earth are they going to reprogram these things when new launch points are used, which did not exist when the `pebbles' were launched?!

Even if they can be made to be reprogrammable, how can anyone be sure that all 100,000 receive the message? And that's even before considering problems like hostile reprogram messages...

Amos Shapir, National Semiconductor (Israel), 6 Maskit st. P.O.B. 3007,
Herzlia 46104, Israel Tel. +972 52 522261

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 36

Wednesday 17 August 1988

Contents

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

Package-deal arguments about VDT's

Philip E. Agre <Agre@WHEATIES.AI.MIT.EDU>
Mon, 15 Aug 88 17:31 EDT

When someone reports on the downsides of a technological artifact, they are often labeled an `anti-technologist'. They are then rhetorically asked if they would prefer a world without electric lights and antibiotics. We might call this a `package-deal argument'. It presents a monolithic entity called `technology' and, by asking `are you for it or against it?', demands either wholesale acceptance or wholesale rejection.

This technique can also be used on a smaller scale. If someone has been injured by working with a computer, one can make a package deal of a monolithic entity called `computers' and say things like, to quote Brint Cooper in RISKS 7(35),

"Risks of using computers must be assessed against the risks of not

> using computers."

Frequently such arguments draw subtly bogus analogies to older, `lower' technologies so as to portray the complainers as irrationally biased against novelty and change. Thus,

> All my life, I have known people who read a great deal in their childhood and wound up with extreme nearsightedness. I knew a chap who repaired small timepieces most of his life and, in his 60's was nearly blind. No one suggested that books and precision repair are risky to one's vision.

Note the monolithic entities called `books' and `precision repair'. Do `books' cause nearsightedness? Does `precision repair' cause blindness? That's not the point. `Books' and `precision repair' don't `do' anything, any more than computers `do' things. What happens when people read books, repair watches, or sit at VDT's depends on the context in which they do it.

When a human being is maimed at work, it is a complex social phenomenon. If `technology' can send people to the moon and keep track of huge inventories, then `technology' can alleviate occupational hazards. Technology is a tool. The point about occupational visual damage connected to employers' workplace practices regarding VDT's concerns the economics of industries that use computers. Do market forces encourage employers to protect employees or to destroy them? The answer to this question has varied at different places and times, but very often the answers have been sad ones.

Cooper is certainly correct that proper epidemiology is required with regard to complaints of eye damage resulting from jobs involving VDT use. I worry, though, that in the context of Cooper's rhetoric, his painfully ironic demand that these studies be `multiply blind', although perhaps methodologically justified, might reflect a worldview in which `technology' is under attack from `anti-technologists' who set up Video Display Terminal Eye Clinics in order to generate pseudo-epidemiological propaganda. This Manichean sort of approach to debates about workplace organization is not going to help in hearing the complaints of the maimed or in making offices and factories into human places to work.

Blue Cube new software problems

Randy Neff <neff@anna.STANFORD.EDU>
Mon, 15 Aug 88 21:13:27 pdt

From San Francisco Chronicle, Friday, Aug 12, 1988. pages 1 and A22
(without permission and condensed)

New Pentagon Satellite System Having Troubles
by John Schneidawind Chronicle Staff Writer

A program to renovate the Pentagon's super-secret "Blue Cube" satellite-control system in Sunnyvale is way over budget and behind schedule, according to a recent congressional report.

The General Accounting Office estimates that the Air Force program's costs,

orignally pegged at about $600 million in 1980, have ballooned to $1.4 billion and could rise an additional $450 million before the project is completed.

The Blue Cube, a top secret computer facility at Onizuka Air Force Base, just off Highway 101 and Mathilda Avenue, controls satellites transmitting the nation's most vital military and intelligence secrets. [also next to Navy's Moffett Field, NASA Ames Research, and Lockheed.]

The GAO report was issued last Friday [Aug 5], but so far has been distributed to only a handful of military experts. The Chronicle obtained a copy of the report.

The project's problems include glitches in computer software being developed to process the tremendous amounts of data generated by communications satellites orbiting the Earth.

According to the GAO report, the new system originally was supposed to handle 5 million bits of data per second, but it will be able to handle only about 1 million.

The project was originally scheduled to be completed in October 1987 and was to have included a facility in Colorado Springs that would help control the satellites.

The arrangement would have allowed Sunnyvale and Colorado Springs to function as backup operations for each other.

But the GAO says software problems have pushed the completion of the project to 1989 at the earliest.

"(The) Defense (Department) considers Sunnyvale to be vulnerable to failures from earthquakes or other threats such as direct military attack," the GAO report notes.

Officials at the Air Force's Space Command in El Sequndo, which oversees operations at the Cube, were not available for comment yesterday. Officials from IBM Corp.'s Federal Systems Division in Bethesda, Md. which built the new computer equipment and software, also could not be reached.

The space shuttle is about to return to service, and the main priority will be to put dozens of military satellites into orbit.

But unless problems with the new satellite control systems are corrected, the extra satellites could create capacity problems that may disruput the Blue Cube's existing satellite control system, the GAO report implies.

The Blue Cube -- so named because it is housed in a turquoise-colored building-- is maintained under contract by Lockheed Missiles and Space Co.

According to the GAO, the facility monitors and controls 54 orbiting satellites that provide critical defense communications, navigation, surveillance and weather information. [more on what satellites do]

However, some of the computer technology used to monitor and control orbiting satellites is more than 20 years old, and the Air Force since 1980 has been trying to come up with a new system.

So great are the problems with the new system that the Air Force has yet to fully test it successfully, let alone make it fully operational, the GAO report states.

As of February 1987, the GAO says, "the new system was averaging only a 69.6 percent success rate in performing satellite contact functions, where 95 percent success is the minimum requirement."

The Air Force has told the GAO that the success rate is now 90 percent.

Zero-balance dunning letter

Jerome H. Saltzer <Saltzer@ATHENA.MIT.EDU>
Tue, 16 Aug 88 10:41:33 EDT

Just in case anyone thought those stories about dunning letters for zero balances are apocryphal, yesterday's mail from Bloomingdale's provided a certifiable example:

> Dear Mrs. Saltzer
>
> A review of your account shows the amount below to be past due.
>
> If you feel that this amount is incorrect, please enclose a remittance for the correct amount and give us an explanation of the deductions on the reverse side of this letter. Otherwise we shall expect payment in full of the amount due.
>
> We would appreciate your prompt attention to this matter.
>
> Thank you.
>
> Very truly yours,
>
> K. George
> Divisional Credit Mgr.
> 212-239-0374
> Amount due $******.00

Since the letter seemed very sincere and it requested prompt action, I immediately called the computer-printed telephone number, and reached a recording, which said, "The number you have reached, 239-0374, has been disconnected. No further information is available about 239-0374."

The people in Bloomingdale's customer service department were profusely apologetic; "That letter should never have gone out." "The credit department moved to a new location about a month ago." Apparently the computer hasn't found out about the move yet, and NY Telephone has already forgotten about it.

Jerry

Chicago Disaster Conference

"Lee S. Ridgway" <RIDGWAY@MITVMA.MIT.EDU>
Tue, 16 Aug 88 11:06:12 EDT

A boxed article in this morning's Boston Globe (8/16/88) noted that the organizers of a conference on disasters, slated for Chicago's McCormack Place in November, had to be cancelled due to lack of interest.

> [UPI in San Francisco Chronicle, 16 Aug 88 quoted the PR firm representative representing the organizers: ``It is absolutely amazing, given the things that have happened recently...'' ``Canceling this is a bit of a disaster itself.'' ... PGN]

Car Electronics sensitive for atmospheric interference

Martin Minow <minow%thundr.DEC@decwrl.dec.com>
16 Aug 88 11:01

From the Stockholm daily newspaper, Dagens Nyheter, 27-Jul-1988. [My quick translation. My notes are in brackets.]

Danger of Sensitive Car Electronics
by Anders Lundqvist

Sensitive automobile electronics may be the explanation of the mystery of "sudden acceleration." Interference in the atmosphere or a poor environment under the hood can be sufficient to affect the electronics so that the car unexpectedly speeds away out of control.

This theory was brought forth by the [Swedish Goverment] Traffic Safety Board [TSV], which is worried about the development of electronics in cars.

"The development can be questioned. What are the needs? The engine compartment is a difficult enviromnent for electronics; and how well are the components isolated?" wonders Bo Jarleryd at TSV.

Mats Gunnerhed, a departmental director at the National Defense Research Institute [FOA -- a Swedish equivalent of Mitre] has studied the problem of sudden acceleration in cars since the summer of 1987. One explanation is, according to Gunnerhed, that the circuitboard for the automatic speed control can be easily damaged [in such a way that the device forces full acceleration. Gunnerhed demonstrated that a break in a single circuit-board trace can cause this problem. There was a note on this in a recent Risks.] ...

But "sudden acceleration" has even been seen in cars without automatic speed controls, which caused TSV to become interested in all electronic equipment. "Scientific reports from Japan show that robots have killed 8 or 9 people because of errors in the electronics. Interference from nearby machines has affected the robot's microprocessors," says Bo Jarleryd.

"The question is how sensitive automobile electronics and their microprocessors are? We have received several reports from drivers whose automatic speed controls have turned off when they are in the vicinity of Arlanda [Stockholm's airport]. This suggests that atmospheric interference in an area with many radio [and radar] transmitters may be sufficient to halt the electronics." [quote not attributed.]

Sudden acceleration cannot be associated with a single brand of automobiles. owever Audi has been associated with a number of accidents where the car has unexpectedly sped away. One accident occurred in Stockholm about two years ago where a car rushed up on the sidewalk and drove over two pedestrians, causing the death of an older woman.

The police examination couldn't find anything wrong with the car.

Nor could anyone in the United States find any technical problem with the 800 cars that were involved in accidents caused by sudden acceleration up to January 1987.

In any case, Audi in the USA decided to recall 250,000 cars in the 1978-1986 model years with automatic transmissions to add an interlock in the transmission that required the driver to step on the brake before putting the car in drive. Even though the problem was, and still is, unsolved.

Even Ford, GM, Volvo, Saab, and Mercedes have had problems since the 1970's.

The American government decided on Monday [25-Jul-1988] to examine a total of 215,000 German-built Mercedes Benz in the 1984-1988 model years with gasoline motors and automatic transmission. This is due to an alarm raised by the "Center for Automobile Safety" on "sudden acceleration" in the cars.

According to the group, 164 reports of sudden acceleration of Mercedes Benz have come in. 125 accidents were reported, resulting in 46 injured and one death.

According to Philipsons, the importer of Mercedes Benz in Sweden, this is primarily the 300E model with automatic speed control.

[I think there's an old Risks item noting a "sport" played by truckers with high-powered CB radios, where they zap cars trying to pass them, causing their electronic fuel injection to fail. Also, note a recent Risks I posted about the recall to fix the automatic speed control in my Volvo.]

[Translated by Martin Minow, minow%thundr.dec@decwrl.dec.com]

---

1 in 10 NATO software modules reported incorrect (COMPASS '88 report)

Jon Jacky <jon@june.cs.washington.edu>
Tue, 16 Aug 88 08:47:06 PDT

I attended COMPASS '88, held June 27 - July 1 at the National Bureau of Standards in Maryland. COMPASS (for "Computer Assurance") is an annual meeting devoted to the safety and security aspects of computer systems.

John Cullyer from the Royal Signals and Radar Establishment (RSRE), the central electronics research laboratory of the UK Ministry of Defence (MOD). gave a paper on his group's VIPER microprocessor, a 32-bit RISC chip designed for safety-critical applications.

The VIPER project fits into a larger computer safety program at RSRE, and Cullyer tried to convince the audience of the necessity for developing systems with a great deal of mathematical rigor. Cullyer explained that RSRE's safety program derived from MOD's concern over the integrity and safety of its computer-based weapons and vehicles. RSRE performed a study of NATO software in the early 80's, using a static analysis technique in which a program is represented as a directed graph, various expressions are associated with the

arcs and conclusions regarding correctness are derived from them. (Several automated tools based on the RSRE work are on the market, including MALPAS from Rex, Thompson and Partners, and SPADE, from Program Validation Ltd. Cullyer said a similar idea was behind an American tool called DAVE). Of the modules (a program is composed of many modules) which RSRE sampled from the NATO inventory, 1 in 10 were found to contain errors, and of those, 1 in 20 (or 1 in 200 overall) had errors serious enough to result in loss of the vehicle or plant! About the same findings were made whether the code came from Britain, the USA, or West Germany.

But the MOD was really roused by several "near-miss" accidents which Cullyer said he was not permitted to discuss. He mentioned in conversation that one incident involving "general ordnance" might have resulted in hundreds of deaths. A military board of inquiry determined that computer problems were at fault. Studies determined that incidents derived with approximately equal frequency from three kinds of problems: incorrect or incomplete specifications, errors in programs, and "unexpected functionality" from microprocessors. This last item came as a bit of a surprise; what it meant was that the processor as delivered simply did not behave as described in its assembly language programming manual. VIPER is an attempt to address this problem. The project was felt to be so urgent that it was funded within 48 hours of submission.

Cullyer closed his talk with a warning: "I don't think we have all pursuaded our bosses that there is a problem. If we do not implement these methods, there will be a lot of accidents and a lot of people will die. If we do implement them there will still be accidents, but we will limit the casualties." He also mentioned that new MOD software procurement standards (which he helped draft) will require formal development techniques for critical software. He added that he thought British law and tradition were more protective of people and sensitive to safety concerns than in the USA. For example, MOD regulations explicitly prohibit any cost saving that might increase hazard to life -- you are not allowed to trade lives off against money.

(This is an excerpt from a report on COMPASS '88 that will appear in the October issue of ACM SOFTWARE ENGINEERING NOTES. The conference proceedings including Cullyer's paper on VIPER are available $30.00 from COMPASS '88, PO Box 5314, Rockville, MD 20851)

- - Jonathan Jacky, University of Washington

Mathematical Error Puts Deficit off by $1.2 billion

Peter G. Neumann <NEUMANN@csl.sri.com>
Wed 17 Aug 88 16:48:47-PDT

WASHINGTON (AP) -- A $1.2 billion mathematical error by the Reagan administration in calculating the size of next year's federal deficit could spark a fight within Congress when lawmakers return to the capital next month. The mistaken estimate, which under the Gramm-Rudman balanced-budget law cannot be rectified, is preventing the spending of $1.2 billion at a time when

legislators are struggling to decide which among several competing spending bills they will pass. ... OMB first made the error when calculating the rate of spending in a foreign military sales program in an August 1987 deficit report... [From the San Jose Mercury News, 17 August 1988]

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 37

Friday 19 August 1988

Contents

- Virus insurance
  Rodney Hoffman
- Blind faith in overly electronic locks
  Leonard N. Foner
- Fewer Charges Now Require a Signature
  Kian-Tat Lim
- Re: Danger of Sensitive Car Electronics
  Hugh Davies
- Info on RISKS (comp.risks)

Virus insurance

Rodney Hoffman <Hoffman.es@Xerox.COM>
17 Aug 88 15:39:55 PDT (Wednesday)

A front-page article by James Daly in the August 15 `ComputerWorld' surveys availability of insurance against computer viruses. Excerpts:

> ... A recent survey of insurers providing computer security policies revealed an industry with not only a dearth of knowledge about viruses but an inability to determine whether policyholders are now or will ever be covered. And at least one underwriter has also begun to specifically reject virus protection....
>
> Even where virus protection is not specifically excluded, an enormous gray area exists. "We're looking into it, but we're not sure it would be covered anyway," said [one insurer]. Others put it more bluntly. "I don't think you'll see coverage ever offered," said [a computer security lawyer]....
>
> At a recent American Bankers Association conference, a speaker from Lloyds of London said the number of outstanding computer crime-related claims would devastate the industry if they were all brought to fruition. And the virus outbreak has made a bad situation even worse....

> Additionally, it has always been difficult to put a dollar value on information, and some assert that if everyone hit by a virus made a claim, the courts would be tied up for eons just figuring out how much the data was worth.
>
> ... The deductible on many [computer security] policies ... often begins at around $10,000, but may skyrocket to $3 million at large banks....
>
> One underlying problem, most underwriters admit, is that they cannot keep pace with changes in the technology.... The Surety Association of America, a quilt of nearly 600 insurance underwriters, has formed a committee to begin reworking some of its policies, and computer viruses "will certainly be on the agenda," said [the assoc. V.P.]....
>
> "We're doing like everyone else: trying to understand the technical aspects of the virus," said [one insurance company senior V.P.]. "Maybe then we will be able to relate it to some coverage."

Blind faith in overly electronic locks

Leonard N. Foner <foner@wheaties.ai.mit.edu>
Thu, 18 Aug 88 00:03:05 EDT

I work at a rapidly-growing company in Cambridge (currently about 160 people) that just recently expanded to the third floor of our current building.

Prior to the expansion, we had a keypad on the first-floor door that would be used to open the door from the outside. To open the door from the inside, you turned a mechanical latch that overrode the electric one (probably a spring-coupled system like many other standard electric latches). The second floor was locked with a completely nonelectronic lock, and is the main entrance for visitors and other such people.

Well. Shortly after we expanded to the third floor, the main door to the space acquired a locking device which was essentially a metal plate bolted to the top of one door in a double door. (The other door just uses the up-and-down slides that lock it in place in the floor and ceiling unless you've got the first door open---you've probably seen the type). When the door with the metal plate is closed, it contacts a very strong electromagnet mounted at the top of the frame that holds the door shut with a theoretical strength of about a metric ton.

This magnet is controlled by a motion sensor mounted on the inside of the space, on the wall to one side of the door. The motion sensor presumably is wired to the central alarm system (i.e., not in series with the actual electromagnet).

Stop and think a moment about the implications of this. Think you've got them all?

It gets better. It turns out that when the system was installed, *no one was told* that there was a motion sensor on the inside. The door automatically

locked at 6pm. Immediately thereafter, somebody tried to get out on his way to the airport, stopped a moment just inside the door to check something on his person, and tried to open the door.

Surprise.

With the magnet on, turning the (unlocked) knob does nothing, because the door is physically held closed. Further, we had someone on the outside (coincidentally) who was trying to get in. What *they* didn't know (again, because the alarm company didn't tell anyone else what they were doing) was that they had to hit the # key on the keypad after entering the combination. So the keypad was essentially inoperable, too.

It turned out that it took about fifteen minutes for us to open the door, from either direction. No one on the inside was moving enough for the motion sensor to notice them (they were pushing on the door, to no avail, or typing on an alarm control panel which seemed dead and was, in fact, not connected to anything). Eventually, someone happened to step back and scratch their head or something, at the same time someone was pulling on the outside of the door, and it magically and mysteriously opened with no effort at all.

No one knew why the door had unlocked, so the person who was now late for the airport departed, while we opened the adjoining door so we could close the magnetically locked one to figure out what was going on without risking being locked in.

It took us another fifteen minutes to finally notice the correlation between movement and the magnet. (Since the magnet turning off is not audible, unlike a latch retracting, we had to park one person leaning on the door to guarantee that we'd know when it opened. And the motion sensor, since it looks sideways across the door, and very high off the ground, is not very sensitive to short or medium people walking *toward* the door.) Another few minutes of work yielded the procedure for the keypad, and we were all set---or were we?

I had had bad misgivings about the magnet from the moment I had seen workmen installing it, and it turns out that they have been borne out. Consider, for example, that there is no switch, not anywhere, that is directly in series with the magnet's power supply. Any failure of the motion sensor, its wiring to the alarm, or the alarm itself could jam the magnet on, with no remedy except unscrewing the (obviously nonmagnetic and probably aluminum) casing of the magnet and cutting the leads. Given that the case has about ten phillips-head screws, I wouldn't like to try this in a fire---especially when you consider how long it generally takes to find a phillips-head screwdriver and a pair of diagonals...

Incidentally, the alarm and the magnet are battery-backed. Even a fire that killed the 120V power would not unlock the door, and if it burned through or shorted, as appropriate, the correct wires, you can guess the outcome.

So once I realized how insanely they had designed the system (what's wrong with an ordinary latch?), I went to our chief administrative officer, who's also in charge of things like alarms, and asked her to put a manual override on the magnet. I drew a schematic to indicate that the switch should be in series with the magnet itself, not

connected to the alarm's logic. It only took *three days* to convince her of the necessity for the change...

I also asked how the fire marshall could possibly approve such a dangerous fire exit. She gave the incomprehensible answer that the alarm people *were* firemen. Since I'm not aware that the fire department routinely double-dips by working as alarm installers in their off hours, I let it drop there. I'll probably ask the fire marshall to come take a look if things don't improve.

So the alarm people, who were initially rather startled that we didn't trust their alarm to work perfectly in all cases, even in the event of a fire, said that asking for a switch wasn't totally a new concept, and installed one (no doubt anything they can charge us a bundle for makes good sense to them). This switch is the sort that is labelled "Pull in case of fire" and generally makes it look like it's a bad thing to pull the switch casually (it looks pretty non-resettable). This makes me hesitant to test it. However, the fact that the switch is on the wall under the motion sensor, rather than between the magnet and the alarm (which is in a room on the *opposite side* of the door from the motion sensor) makes me believe that the switch is simply in series (or parallel, if it's normally-open) with the motion sensor. This removes one point of failure (the motion sensor), but still leaves all of its wiring and the central alarm's logic circuits, which have already (in two weeks of operation) demonstrated themselves to be unreliable. (No one could get in on Saturday. The alarm company insisted that the logic had gotten wedged because someone had entered their combination "too quickly" on the keypad outside. I don't know whether to believe them---and assume that the engineer who designed the alarm is incompetent---or disbelieve them---and assume that the maintenance guys are incompetent. Neither is very reassuring in the face of this non-overrideable lock.)

So we're left with a system that is difficult to test (sometime late at night I will almost certainly disassemble the various pieces to see where the wires go, and thus where the switch is in the circuit), unfriendly (the motion sensor is not very sensitive, requiring people to often walk back and forth, jump up and down, or wave things to get out), insecure (sticking a piece of paper on a coat hanger between the gap in the two doors and waving it vigorously enough should open them, if it's a sufficiently large piece of paper), and dangerous (multiple points of failure all leading to being locked in).

Whatever became of good, old-fashioned mechanical locks?

To top it off, the second floor just got an electronically controlled latch (not an electromagnet, but again with no obvious mechanical override), and it, too, is attached to a motion sensor...

Fewer Charges Now Require a Signature (L.A. Times)

Kian-Tat Lim <lim@csvax.caltech.edu>
Fri, 19 Aug 88 00:29:09 PDT

Fewer Charges Now Require a Signature
By Albert B. Crenshaw, the Washington Post

Los Angeles Times, August 18, 1988, page IV-3

WASHINGTON - A hotel in Richmond, Va., discovers some telephone charges after a guest has checked out. No problem. An employee telephones the guest and tells him the hotel will simply put the charges on his credit card.

A restaurant in Washington demands a credit card number when taking reservations. If the guests fail to show, a $15 charge is placed on the credit card.

A busy professional spots an appealing item in a catalogue, dials an 800 number and says, "Ship it and put it on my credit card."

These transactions, like millions of others in today's charge-it world, have one thing in common. A charge was recorded on a credit card but no signed document changed hands.

Signatures Not Required

The signature, in fact, is rapidly becoming obsolete in credit card transactions.

Having a customer sign a slip when he or she buys something is already "less significant than it was" in the past, said Dan Brigham of Visa International. Credit cards today are evolving into "a national payment system," said Spencer Nilson, publisher of the Nilson Report, a California-based newsletter that tracks the credit card industry.

"It allows you to do things you cannot do with cash," such as make long-distance transactions, Nilson said. "That is what people pay interest for, what they pay fees for," and as the system becomes increasingly electronic "the trend is for more transactions to be without signatures," he added.

"Nothing in the law specifically requires a signature" in a credit card transaction, said Elgie Holstein of Bankcard Holders of America, a Virginia-based consumer group.

"The issue is positive identification of the card member," said Philip Riese of American Express. This can be done several ways -- by comparing the signature on the card to the one on the charge slip, by using a personal identification number similar to those for automated teller machines, and by "what is known generically as 'signature on file,' " Riese said.

In the third case, which arises mostly in telephone transactions, the burden is on the merchant to ascertain the cardholder's identity, though American Express helps by providing an address-verification system that matches the cardholder's address against the one to which merchandise is to be sent.

In some cases signatures are being dropped for in-person transactions, especially where signing a slip may be viewed as an impediment to a speedy sale.

For example, Visa and Arby's, the roast beef chain, are experimenting with putting fast food on plastic. In an effort to keep the fast food fast, they require no signature for purchases under $25.

The clerk merely "swipes" the customer's Visa card through a magnetic stripe reader, which checks a "hot sheet" to see if the card is OK. If it is, then the customer is on his way.

The experiment promises to put fast food where mail order and other forms of remote marketing have been for years. The appeal to these marketers is obvious. Customers enjoy the convenience and merchants find they are able to capture more impulse business -- sales that would be lost if the buyer had to write out a check and mail it in.

While acknowledging the convenience, hover, many customers feel just a bit

nervous at this "loosey goosey" system, as Holstein termed it, of telephone and other signatureless transactions.

But lawyers and others who follow the industry agree that it is the merchant and the card issuer that bear the bulk of the risk.

Under the Truth in Lending Act, consumers are generally protected from losses of more then $50 due to unauthorized use of their credit card. And in practice, said Holstein, the customer's chance of successfully disputing a charge "is in fact enhanced when they don't have your signature."

The law specifically states that if a card issuer seeks to collect a disputed charge, "the burden of proof is upon the card issuer to show that the use (of the card) was authorized" by the cardholder, he added.

Visa's Brigham said that, if a cardholder swears in an affidavit that he did not authorize a disputed transaction, "that's generally the end of it."

This does not mean, however, that there is no risk for the cardholder.

Nilson noted that fraud by "telemarketing" is increasing rapidly and that these thieves prey particularly on those who are not aware of their rights or who may for some reason be unwilling to assert them.

Many of these scams are aimed at merchants by crooks who collect card numbers, run up a lot of charges and quickly skip before the cardholders begin to complain.

But other are aimed at the cardholders themselves.

Nilson said purchasers of pornography offer a fertile field for such scams. Some thieves even make deals with pornography sellers to buy the right to collect their credit card accounts. They then run up phony charges with the numbers.

Often, he said, cardholders pay up for fear that any dispute would reveal what they had been involved with.

In other cases, cardholders may find the issuer willing to go to court with even marginal cases if the amount involved is large enough.

In addition to being a payment system, credit cards are on their way to becoming a national identity card system, as anyone who has tried to check in to a hotel recently can attest.

Businesses that use credit cards as identification are "trying to confirm who you are, that you're not a phony," Nilson said. They regard the credit card "as sort of a monitor. If you don't have one it doesn't mean you're rejected but it triggers something else," such as requirement for further identification.

Re: Danger of Sensitive Car Electronics

<"hugh_davies.WGC1RX"@Xerox.COM>
19 Aug 88 06:52:54 PDT (Friday)

1) In the UK, there is a an area where two large motorways (freeways) converge (the M1 and M6) near Rugby. This area also contains 2 large radio transmitting stations - the BBC transmitter at Daventry and the Home Office transmitter at Rugby (which transmits the MSF time standard, among other things). This area is renowned for the failure rate of electronic engine management systems, which upon the cars involved being towed from the area prove to be perfectly functional. As a result, local car dealers have named the area 'the Black Triangle'.

2) The radio literature is full of instances of interference with car control systems by radio transmitters mounted in the vehicle. My last car would quite happily sound its 'seat belt warning' upon every tranmission on certain frequencies. I have also set off at least one shop (store) burglar alarm whilst transmitting when outside the shop.

The phenomenon of EMC problems (Electromagnetic Compatibility) is well known in the radio, computer and communications industries. There is a large short-fall in the numbers of EMC engineers available in the industry, and in the case of the UK, there are no egress regulations anyway, which leads to a total lack of interest among manufacturers of electronic equipment. The fact that poor egress specifications also lead to poor ingress specifications also seems not to bother the manufacturers of cars, computers, radios, TVs, VCRs, etc. The EEC, through the CEPT, is about to enact an ingress specification, but it is to a very low standard, mainly aimed at preventing interference by CB. The FCC standard appears to be much better, and, by European standards, reasonably well enforced.

Many digital electronics engineers are poorly trained in analogue electronics, and may not realise the magnitude of the problem. It is quite possible for the amounts of RF induced by proximity to radio transmitters to reach the Volt level, at significant currents. There are well documented problems with systems adjacent to multi-megawatt radio transmitters, such as those ecperienced in the national stadium in Jeddah. Most microcomputers are poorly, if at all screened in this respect - they are usually housed in plastic enclosures. Whilst the car is probably one of the most hostile environments known to engineers, it is quite possible for it to become more hostile yet in the prescence of large amounts of RF.

Hugh Davies.

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 38

Monday 22 August 1988

Contents

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

British vs American safety rules

<attcan!utzoo!henry@uunet.UU.NET>
Fri, 19 Aug 88 23:51:36 EDT

> ... He added that he thought British law and tradition were more
> protective of people and sensitive to safety concerns than in the USA. For
> example, MOD regulations explicitly prohibit any cost saving that might
> increase hazard to life -- you are not allowed to trade lives off against
> money.

Britons should not consider this reassuring; it is, in fact, alarming.
This rule was obviously written by a politician (possibly not an elected
one or a recognized one, mind you...), not by an experienced engineer.
It is *always* necessary to trade lives off against money, because there
is no limit to the money that can be spent adding more 9's on the end of

99.9999% reliability. What this rule is doing is guaranteeing that the risks and tradeoffs will not be discussed openly!

Consider what is likely to happen. Manufacturers, under pressure to keep costs under control, will quietly and privately evaluate the tradeoffs. Since they are forbidden to introduce changes that increase hazards, yet may need to make changes as the customer (the government) shifts its priorities around, the obvious thing to do is to start out with the cheapest and *most hazardous* version. If this can be gotten past the inspectors somehow -- nobody should be surprised if manufacturers are less than completely open about hazard analyses! -- then with luck, all further changes that affect safety can be in the direction of improved safety. At higher cost, of course. Assuming that it can be funded in that year's budget, of course.

Is this rule really serving its intended purpose?

Henry Spencer @ U of Toronto Zoology

Another boundary case bug

<Tom.Lane@ZOG.CS.CMU.EDU>
Sun, 21 Aug 88 16:19:35 EDT

Just in case you thought this kind of thing no longer happens in 1988...

The Pittsburgh city water authority just switched over to a new billing system. My first new-format bill reads as follows:

Previous reading: 988 (thousand gallons)
Current reading: 2
Amount used: 0

Sure enough, all customers whose meters "wrapped around" during the past quarter received minimum bills. "We didn't catch it until after the first batch of bills went out," according to the customer assistance person I spoke to. Those customers who don't call in to ask about it will not be billed for the difference until next quarter; the difference in my case was only about $20, but I suspect that the authority may lose a good bit in interest overall.

I find it interesting that the bill wasn't for -986K gallons. Perhaps the programmer actually thought about the case current reading < old reading, and concluded it would always represent a reading error; or maybe it's just a byproduct of some data format declaration.

tom lane

Retired couple jolted by $5 million electric bill

attcan!lsuc!dave@uunet.UU.NET <David Sherman>

Sat, 20 Aug 88 00:00:07 EDT

TAMPA (AP) - A retired couple got a jolt from their July electric bill -- $5,062,599.57 U.S. An offer by Tampa Electric Co. for them to pay "budget" monthly instalments of $62,582.27 didn't help. Company officials apologized to Jim and Winnie Schoelkopf after the mistake was blamed on a computer operator. The correct bill was for $146.76.
[from the Toronto Star, 29 July 1988]

Hotel could get soaked in lawsuit?

Don Chiasson <G.CHIASSON@DREA-XX.ARPA>
Mon, 22 Aug 88 14:03:27 ADT

> Faulty Bath Shower Blamed for Air Crash
> From Canadian Aviation, Aug 88, p. 8
>
> A U.S. pilot has sued the Marriott hotel chain for $7 million, claiming that he was struck in the head by a faulty shower head, causing a flashback nine months later that led to the crash of his helicopter. Joseph Mendes claims that Marriott was negligent because he was injured when struck by a pulsating shower head that came loose and fell on him in 1987 when he was staying at the Marriott hotel in Lexington, KY. Mendes says that he "has suffered a psychic [sic] trauma known as and referred to as post-traumatic stress disorder which is continuing in nature." His suit alleges that "as a direct and proximate result" of the alleged disorder, Mendes suffered a flashback while piloting a helicopter last March, "thereby losing control of the helicopter and causing it to crash to the ground."

What has this got to do with computers? Without knowing more about the incident, I have some difficulty in seeing a *falling* shower head as being a "direct and proximate" cause. If businesses and individuals must defend themselves from suits such as this they will have to keep detailed records of any incident that happens to a customer or visitor. Did the incident happen how, when and where he claims, and if so did he report it promptly? Such records are most likely to be kept on computers. What are the implications for privacy?

> [The usual privacy problems exist. More significantly, the trustworthiness of computer evidence is always in doubt. It is too easy to fudge the data subsequently, even in the presence of time-stamps, cryptoseals, etc. (The most serious problem is probably the increase in frivilous lawsuits.) PGN]

RISKS contributions [I try to sun-dry sundry messages...]

Peter G. Neumann <Neumann@KL.SRI.COM>
Mon, 22 Aug 88 14:28:45 PDT

The backlog of contributions is enormous, but the topics and subject material are really rather marginal. There are at least 15 messages on VDTs (eyes, backs, eyesight changes, etc.), and scads on the use of signatures, credit

cards, vending machines, and on into the night. Much of it has drifted widely from computer relevance, coherence, nonrepetitiousness, etc., and so I am inclined to suggest we all take a rest for a while until some more exciting material materializes. I get more hate mail when I let marginal stuff through than when I don't, so perhaps I'll try to keep the standards up.

Risks of CAD programs

<ark%hoder@CS.RIT.EDU>
Mon, 22 Aug 88 10:12:09 EDT

My father has worked as a civil engineer for forty years. Recently I had a conversation with him on how civil engineering design methods have changed since when he started, especially with the recent widespread use of CAD programs. This made me think of a RISK in using such programs.

He described his latest design project. A vacuum vessel had a large circular opening that was covered with a flat plate. The plate needed to have several irregular holes at odd positions, for mounting pieces of equipment. Since one side of the plate was under vacuum, the plate bulged inwards, destroying the alignment between the mounted pieces of equipment. His task was to design a set of stiffening braces to control the bulge.

In the "old days," he said, a plate with stiffening braces and irregularly-placed holes would be impossible to analyze. It would have been easy to determine the amount of bulge for a plate with braces but _without_ holes, or with, say, one circular hole in the plate's center. In fact, he could look up the solution in any standard textbook. The holes would increase the bulge, but to an unknown extent. He would have made a guess at the amount, thrown in a generous safety factor, and designed the braces accordingly.

Nowadays, he uses a computer program (NASTRAN) to do finite-element analysis. He built a model of his plate, holes and all, ran the machine for x minutes, and found out exactly where and how much the plate would bulge for a given vacuum level. He then knew just how much stiffening would be needed.

Now for the RISK. With a detailed picture of the exact stresses and deflections on a particular structural member, the engineer can justify designing with a smaller safety margin. No longer are large safety factors needed to compensate for the inability to do exact analysis. Instead, one can design with a smaller margin and reduce the cost (fewer or smaller braces are needed).

Do practicing civil engineers reduce their safety margins these days because they use computer-aided analysis? How much? How small a safety margin is small enough? How well-validated are the structural analysis programs in common use? Do they always give accurate answers? Do engineers include in their safety margins any consideration of inaccuracies or bugs in their programs ("I'd better add x% in case my program's results are off")? I'd appreciate hearing from anyone who knows.

Alan Kaminsky, School of Computer Science, Rochester Institute of Technology

Can current CAD/simulation methods handle long-term fatigue analysis?

<attcan!utzoo!henry@uunet.UU.NET>
Wed, 17 Aug 88 23:23:56 EDT

>... Are current supercomputer simulation methods capable of
>handling the complexity of long-term stess, fatigue, corrosive environments,
>etc., all of which were (apparently) factors in the Aloha incident? Also I am
>not at all sure that such things were handled any better before wide-spread use
>of CAD -- I am just asking the question. Any aeronautical engineers out there?

Well, I'm not an aeronautical engineer, but maybe I'll do... :-) As I understand it, metal fatigue in general is poorly understood, and there is really no way of calculating it. The whole area is still very much rule-of-thumb engineering plus empirical testing. There are rules that give a rough idea of the fatigue life of an airframe, after which a big safety margin is added (we're talking factor of 2, not 10%). Even this is only a tentative number. Most any large, volume-production aircraft will have one of the early prototypes shunted off into a corner to be the "fatigue test" specimen, which means that it spends years (literally) having its wings bent back and forth and pressurization cycled up and down and generally having stresses applied in a speeded-up, exaggerated simulation of real service life. The objective is to keep the fatigue-test aircraft well ahead of all the real ones, while watching it carefully for signs of fatigue cracks.

Even so, one still gets surprises. Not just the occasional accidents, but also more mundane discoveries of cracks; fatigue-life estimates are not trusted very much, and aircraft are inspected regularly. Now and then such an inspection yields a surprise, and the manufacturer or the FAA sends the other users of that aircraft a telegram saying "inspect area XXX right away and let us know if you find cracks". This seldom makes the news, but it happens with some frequency.

I guess this is not a bad example of how to manage a poorly-known risk...

Henry Spencer @ U of Toronto Zoology
uunet!attcan!utzoo!henry henry@zoo.toronto.edu

Vincennes and Cascaded Inference

<CFEEHRER@G.BBN.COM>
16 Aug 1988 07:32-EDT

Thank you for the comments and interest in the cascaded inference notion. As a newcomer to the Comp.Risks forum, I judged that the Bayesian approach to decision making, if not cascaded inference, per se, had probably been kicked around before, and I didn't quite know quite where to start. I'll try here to be a little more crisp in my arguments and provide some references to the general area. When I have something better than this 300 baud connection,

maybe I can push on!

First ... to get some of the fuzz out of the earlier arguments!:
(Please note that I am indebted to Clifford Johnson -- 11 Aug -- for forcing me to make some of the assumptions clearer.)

(1) Although the Vincennes affair provides fertile ground for the imagination, little enough is available in the common media, my only source, to get any kind of closure on the validity or truth of assertions. After Seymour Hirsch writes a book, I'll feel more comfortable with any position I take! I'm drawn to the case only because I think it is altogether likely -- and I think newspaper reports bear it out so far -- that not all of the information that could have been brought to bear on the decision was used, and some of the information that was used was "noisy" in ways that could have misled decision makers if they didn't have means for coping with it.Those characteristics can be identified in almost any post-analysis of a complex decision situation, whether things went well or badly, and I take it on faith that they can be found here. To observe them again would be almost trivial if it were not for the fact that their ubiquity argues, at least to me, that we had better soon figure out how to mitigate their impact.

(2) I DO NOT want to argue that crucial decisions should be automated, except where human and/or system response times are so long that non-automated decisions are impractical. I DO want to argue that decision makers should be taught how to make the best use of all of the information they have and then be provided with the best computerized aids to diagnosis and inference that we can devise. I think we put individual decision makers, whole systems, and maybe the entire world at risk if we do otherwise.

(3) We need to keep in mind that "hit" and "false alarm" rates are inextricably associated. If one MUST avoid a Stark, then one will occasionally have a Vincennes. There is no level of system perfection that can, in principle, destroy that association. Ironically, it may be that, unless we are very careful in their design, the more complex our systems are made to be in the interest of greater accuracy, the more false alarms may ocur and need to be dealt with.

(4) I have little interest in defending Bayes Theorem or, for that matter, any particular method of statistical inference (e.g., Neyman-Pearson methods). We know pretty well the limitations of probabilitic statements in the context of low frequency events. (Or even high frequency events, for that matter: "So the probability of rain is .6! Do I take the umbrella or not?!") And I certainly don't want to suggest that military commanders and CEOs and surgeons should sit around with calculators and compute posterior odds, F-ratios,ts, etc. If it makes any sense to do that, it should be done automatically as part of a computer-based decision support system!

I DO want to suggest that the Bayesian model, and to a lesser extent, classical N/P models, have been extremely useful in highlighting the fact that human decision makers do not typically extract from data, whatever their quality, as much information as is justified. On some occasions, that "shortcoming" results in the need for more data to be acquired and processed, thus incurring additional costs in resources and time. On other occasions, particularly if time is critical, it can result in the choice of an incorrect hypothesis.

Now, there are two questions concerning that finding: Why?, and What can be done about it? I'd like to contribute some stuff on those questions and get your reactions, but it's a big topic and a digression at this point. If anybody is interested, HOLLER!

(5) I agree thoroughly with CJ that there is a welter of data and no "unequivocal attack warnings" (until a hostile action has been taken) -- that's precisely why it's an interesting problem.A few years ago, several colleagues and I were studying (with their cooperation) the decisions of nuclear power plant operators who were on duty at times during which plant instabilities occurred and who, for considerable periods, were in doubt about what had gone wrong and what the current states of their plants were. Two of these instabilities had resulted in radioactive releases. If you've been in a plant when things start to go bad, you know something about the enormity of data that suddenly comes your way, the confusion and tension it can produce, and how critical it can be that things get figured out quickly and correctly ... you don't simply "turn it off" and fix it later! I think the operators on Vincennes must have endured a very similar situation.

(6) I can also agree that (a) Captain's role (could) be reduced to "second-guessing" the computer, although I know too little about SOPs in this case to have much confidence in that judgment. (If the system is built that way and the SOP reads that way, serious mistakes have been made. Similar problems have arisen in the design of advanced tactical and commercial aircraft and have become real concerns.) I disagree that there is a moral issue in second-guessing so long as there is total uncertainty and a guess is truly called for. I believe that there are moral issues in this whole thing but that they lie elsewhere.

(7) I still have difficulty, in principle, with the argument that there cannot be (should not be?) decision thresholds (or decision criteria, if you will). Ultimately, there must be the decision to shoot or not to shoot, to buy or to sell, to cut or not to cut, to render a guilty or a not-guilty verdict, etc. In any of these situations, of course, one can almost always defer action in the hope that more information may become available and clarify the issue. But that choice is usually not without cost and, eventually, a course of action must be taken that is based on what can be inferred. A criterion for that decision MUST be defined. For me, it is not the concept of "threshold", per se, but our inabiliity to help the decision maker understand whether or not it's been reached and/or whether it CAN be reached given the validity, and reliability of the available data that presents the problem.

There are some interesting data on the ordering of radiological tests that bear on the this last point. Namely, it can be shown that, in order to be "perfectly sure", some physicians may order tests to be performed that could not, under the very most favorable circumstances, produce increments in confidence great enough to affirm or disaffirm their preliminary diagnosis. A reason seems to be that many are untrained in the utilization of the "yield" statistic -- a quantitative estimate of false positive and false alarm rates based on experience and generally available for standard diagnostic tests. For this knowledge may be substituted a naive belief that if enough tests are performed, the truth will out (before the patient packs it in!).

(8) Here are some initial references on the cascaded inference stuff. Some may be hard to find, so I'll provide some Xeroxed pages from the last reference if you drop me a SASE. The pages summarize some of the arguments in the references:

The earliest paper I'm aware of that sets the stage for a prescriptive approach: Dodson, J.D. Simulation system design for a TEAS simulation research facility. Report AFCRL 1112 and Planning Research Corporation, LA, Nov. 15, 1961.

A very concise/well-written statement of a Bayesian prescriptive approach (my favorite!): Schum, D.A. and DuCharme, W.M. Comments on the relationship between the impact and the reliabiliity of evidence. Org. Behav. and Human Perf., 1971, 6, 111-131.

Examples of attempts to provide empirical models of what untrained DMs actually do: Snapper, K.J. and Fryback, D.G. Inference based on unreliable reports. J. exp. Psychol., 1971, 87, 401-404.

Gettys, C.F., Kelly, C.W., and Petersen, C.R. Best guess hypothesis in multi-stage inference. Org. Behav. and Human Perf., 1973, 10, 364-373.

Funaro, J.F. An empirical analysis of five descriptive models for cascaded inference. Rice Univ., Dept. of Psychology Research Report Series, Report No. 74-2, May 1974.

A different approach, inspired by Bayesian thinking but developed within the signal detection framework and applied to medical diagnosis (references in here are also useful) -- Swets, J.A. and Pickett, R.M. Evaluation of Diagnostic Systems: Methods from Signal Detection Theory. New York: Academic Press, 1982.

Nickerson, R.S. and Feehrer, C.E. Decision Making and Training: A Review of Theoretical and Empirical Studies of Decision Making and Their Implications for the Training of Decision Makers. Tech. Rept. No. NAVTRAEQUIPCEN 73-C-0128-1, August, 1975.

That's a start. Maybe I can sort through the many others and make recommendations if we really get into this area. Some are fascinating!

--Carl

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 39

Wednesday 24 August 1988

Contents

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

Computers and Gambling

George Michaelson <munnari!ditmela.oz.au!G.Michaelson@uunet.UU.NET>
Wed, 24 Aug 88 13:22:23 +1000

"GAME BANDITS FOIL POLICE" (`Australian' computers section, 23 August 1988)

Victorian & N.S.W Police are noting an increased use of "bent"
one-arm-bandits used to finance drug & other big-money crime.
The head of the racing and gaming squad reported machines that:

"..appear to run legitimate amusement games but with the flick
of a switch they are converted to gambling machines.

Machines of greater sophistication are now starting to appear
with a second switch that totally erases the computer program

[sic] which runs the illegal games.

If that happens we are powerless to prosecute."

George Michaelson
CSIRO Division of Information Technology 55 Barry St, Carlton, Vic 3053 Oz

---

Car engines become target for hackers

George Michaelson <munnari!ditmela.oz.au!G.Michaelson@uunet.UU.NET>
Wed, 24 Aug 88 13:34:54 +1000

Extracts from the australian of 23/8/88:

Computer hackers have found a way to make cars go faster. They are breaking into tiny engine management computers and reprogramming them to give family cars extra acceleration.

One large motor company is about to fit a secret detector "to foil hackers and safeguard used car buyers from being duped".

Computer tweaking can seriously damage a turbocharged engine, particularly if it is driven on "full boost: over a long stretch of road; and there are "growing signs of fraudulent warranty claims" an industry official says.

It costs about $800 to have the engine computer tweaked by specialist hacking-tuning companies. There are alternative go-faster computer chips ready to be installed while you wait. Customers include owners of every computer-controlled car in the book. Computer buffs can do themselves for about $20.

Motor companies are now planning to guard themselves against warranty claims that might arise through unauthorised computer up-rating resulting in engine failure. The new electronic detector will record a cars computer instructions when the vehicle is brought in for breakdowns to be repaired under warranty. False instructions will be detected and the owner told the change has invalidated the guarantee.

Insurers say the unauthorised modifications will invalidate the insurance policy.

George Michaelson, CSIRO Division of Information Technology

> [Early issues of risks have addressed this problem in the USA. For example, RISKS-4.12 noted the reprogramming of an 1984 Firebird. PGN]

Vincennes and Non-Computer Verification [CFeehrer RISKS-7.38 (and 33)]

David Collier-Brown <daveb@geac>
Wed, 24 Aug 88 10:12:23 EDT

One point that I did not see in the discussion to date (which CFeehrer inadvertently reminded me of), was the peculiar position of the Captain of the Vincennes: He had no independent means of verifying the correctness of the information his battle-management system was using.
He was faced with making a decision with doubtfull information, information which did not become "better" over time, and before a certain time, after which it would be too late to defend himself against an aircraft and he would have the greater risk of defending himself against a missle.
Not a good situation to be in.

Yet it is a perfectly "ordinary" consideration in war to try to verify the poor, incomplete and fragmented information which a commander has to deal with. If your air force says an enemy column is near, you send out a scouting force to verify that this really is th enemy you're worried about (and to slow it down if it is). If your radar says a bear bomber is approaching the coast of Labrador, you send out aircraft to have a look, and hopefully send the bear on its way.
In the case of the Vincennes, where was the air patrols which should have accompanied any major combat vessel? Where was the captain's eyes and first line of defense against air attack?
Even in peacekeeping operations, one tries to have sufficient support arms nearby and available on a moment's notice (SOS tasks if they're artillery, combat air patrols if they're air force, etc.)

Indeed, **what happened** in the case of the Vincennes? Was the U.S.operating naval patrols in a war zone without air support? If so, why?

What kind of faith are we placing in electronics if we send major vessels out "alone" into war zones, even on non-warlike missions, without providing them with mobile forces to identify and hopefully deal with air attacks, and nearby support forces for backup?

David Collier-Brown, 78 Hillcrest Ave, Willowdale, Ontario
{yunexus,utgpu}!geac!lethe!dave

Shades of War Games (Source passwords)

<SPGDCM%UCBCMSA.Berkeley.EDU@jade.Berkeley.EDU>
Tue, 23 Aug 88 16:45:27 PDT

I just received a mailed promotional piece from The Source, a well-known info network. It included an application form.

To my astonishment, it included a blank for "Mother's Maiden Name (for verification of ID or Password if lost):_____".

Good Heavens! This implies that a publically obtainable, permanent fact about me could be used to obtain my password, or equivalently, that this factoid IS in effect my password regardless of what I select. Need I say more?

[Surprised? PGN]

Emissions testing risk

<att!ttrdc!levy@ucbvax.Berkeley.EDU>
Tue, 23 Aug 88 00:16:20 PDT

In the Chicago area, for the last two years, there has been a program of auto emissions testing, administered by the IEPA (Illinois Environmental Protection Agency). Auto, truck, and van owners here are required by law, upon mailed notice, to bring their vehicles annually to special testing stations. At a testing station, an attendant puts a sensor probe in a vehicle's tailpipe; the driver idles the engine at low and high speeds, and the machinery checks the pollutant emissions. When the test is finished, the attendant keys in the car's vehicle identification number (read from a pre-test windshield sticker that is peeled off) and the results are recorded in an IEPA computer database.

If a notified vehicle owner neglects to have the vehicle tested (or fails three tests in a month and does not qualify for a waiver by having certain required service done on the vehicle) the owner will be sent a series of followup notices over several weeks. If these are not heeded, the vehicle owner's driver's license is suspended and this fact recorded in a police data base. The owner becomes liable to arrest should he or she drive while the license is suspended and be ticketed or stopped for even a minor traffic offense.

Personally, I believe in emissions control and emissions testing (how could I say otherwise after the stand I recently took in rec.autos? :-) but, of course, the computerization of the system is liable to the usual snafus we all know and love to hate. As printed in the Sunday, August 21 Chicago Tribune headline article, "100,000 drivers risk jail under clean-air law" (almost all of these are because of genuine negligence to obey the law, rather than computer foulups, but this is still pertinent to RISKS):

> ... Joel Aaseby of Elmhurst ... was issued a traffic ticket following a minor accident in Elmhurst. "They ran my name through the police computer, and there was the notice of my suspended license," Aaseby said. "... I had to go down to the station under arrest and fill out a bond card."
>
> What made Aaseby's experience upsetting for him was that he had passed the auto emissions test, but in the process one of the testing clerks punched the wrong vehicle identification number into the computer. Aaseby got several more notices that he had failed the tests and that his license was about to be suspended. "Numerous times I mailed them [the secretary of state's office] all the documentation that I had passed, but never heard back until I was arrested," he said.
>
> "Now I have a court date, and I will take my documentation to court and I'm confident the judge will understand, but do you have any idea how much aggravation I have gone through, especially since the news- paper listings of arrests has my name on the top of the list this week for driving with a suspended license?" he said.

> "We have heard these kinds of stories," [Cinda Schien, Illinois EPA spokeswoman] said. "But hopefully we have got [sic] rid of these problems. We think we are fortunate we haven't had more. "Remember, we are dealing with 2.5 million cars and numerous mailings for each one. We basically had to invent the wheel for the first couple of years," she said.

What bothers me the most about this is not the foul-ups themselves (there are almost bound to be problems in any massive endeavor of this sort) but rather the apparent refusal of the people administering this system (and the associated law enforcement system) to take full responsibility for foulups when they do happen, and their apparent propensity to believe they're not really happening. Why else, for example, would Schien have spoken of "hav[ing] heard these kind of stories" instead of something like "being aware of occurrences like this"? Do I smell some bureaucratic CYA here?

Re: British vs. American safety rules

Jon Jacky <jon@june.cs.washington.edu>
Tue, 23 Aug 88 10:02:20 PDT

<> (I reported) (British Ministry of Defense) regulations explicitly
<> prohibit any cost saving that might increase hazard to life -- you
<> are not allowed to trade lives off against money
>
> (Henry Spencer replied) Britons should not consider this reassuring;
> it is, in fact, alarming. This rule was obviously written by a politician
> ... not by an experienced engineer

Cullyer said that he himself had a hand in drafting some of these MOD regs, although he didn't go into detail about who wrote what at the level of chapter and verse. Whoever was responsible, Cullyer was clearly approving of this particular requirement. He is certainly an "experienced engineer" - - and evidently a good one; several people at the conference (including our moderator, Peter Neumann) said the VIPER work appeared to be the greatest practical achievement yet made in the formal verification field.

> (Henry asks) is this rule really serving the intended purpose?

I should emphasize that Cullyer was not reading verbatim from the rulebook - this was his verbal paraphrase of the intent of the regulations. The point Henry makes - that you can ALWAYS propose some change that appears to increase the safety but also increases the cost - does require a response. I can only say that Cullyer and his group appeared sharp enough so that I assume this was dealt with in some reasonable way. I gathered from the context of what he was saying that the intent of the rules was that shortcuts should not be taken to meet schedules or budgets if these resulted in violations of accepted standards and practices - and that these standards should be kept high.

> What this rule is doing is guaranteeing that the risks and tradeoffs
> will not be discussed openly!

In fact Cullyer, who is an employee if the British MOD, gave a franker description at a public meeting of software problems within his organization than I have ever heard in public from any employee of the United States Department of Defense (or any other public or private organization, for that matter). I am not aware of any United States studies like the NATO software study, in which samples of software from the field were systematically examined for latent faults, prior to any accidents - and then the results were reported at a meeting in a foreign country. I emphasize that Cullyer's presentation did not have the connotations of aggrieved victimization usually associated with "whistleblowing" in this country - rather the RSRE group and the MOD administration were engaged in a constructive effort to be as thorough as possible.

> (Henry suggests we) consider what is likely to happen. ... Manufacturers
> will privately evaluate the tradeoffs - the obvious thing to is to start out
> with the cheapest and *most hazardous* version.

I understood Cullyer's larger point about the difference between the two countries to be that the climate in Britain is such that the pressures encouraging this kind of adversarial legalistic maneuvering are somewhat less than in the US. I would add my personal observation that if Cullyer is any example, British civil servants are afforded higher status and respect than many of their counterparts in the United States, therefore manufacturers realize that the reviewers who evaluate their products may be at least as smart as they are, and will recognize ploys such as the one Henry describes.

I think Cullyer's point regarding the regulations was that it is possible to do a better job at designing safe computer-controlled equipment than is now common practice. It need not even be all that much more expensive, but people do not do it because they do not know how, or are unwilling to expend any additional effort. He noted that it took a certain amount of goading from people in authority to make the point that safety should be an important design goal, and that a good way to do that was to announce that products found wanting will be rejected.

I also understood Cullyer to mean that when designing things like fly-by-wire aircraft, nuclear weapons fuses, and nuclear power plants, it was necessary that a degree of goodwill and cooperation exist among all parties, and that excessive attention to cost-cutting would just get everyone into big trouble; if the budgetary pressures are all that pressing, the project should perhaps not be undertaken.

> It is *always* necessary to trade lives off against money, because there
> is no limit to the money that can be spent adding 9's to the end of
> 99.9999% reliability

Interestingly, another of Cullyer's points was that statistical reliability estimates with lots of 9's in them were not meaningful, and he did take personal credit for writing the MOD regulations that say that such claims will not be regarded seriously! Actually several speakers at COMPASS made this point. It is discussed at some length in the report that will appear in the October 88 ACM SOFTWARE ENGINEERING NOTES, and I will post an excerpt to RISKS.

- Jonathan Jacky, University of Washington

Re: Structural analysis programs (RISKS-7.38)

Stephen D. Crocker <crocker@tis-w.arpa>
Mon, 22 Aug 88 17:57:51 PDT

Alan Kaminsky suggests detailed structural analysis programs, e.g. NASTRAN, are making it possible for engineers to justify smaller safety margins, and he asks in various ways if this represents a RISK.

This reminded me that current practice for design and implemention of software has a complementary RISK. It is quite common for computer system designers to select hardware that has more memory and speed than they think they're going to need. "Safety factors" of two to four are often considered reasonable if they don't increase the cost too much. However, this safety margin usually has far less basis than a NASTRAN analysis, and the results are often expensive. Sometimes the slack is consumed during implementation when it's discovered that the program just doesn't run as fast as it was expected to, and sometimes the slack is consumed during operation. It is not uncommon for simple "data overrun" conditions to lead to software crashes because the programmer never expected the input to exceed the computer's speed.

The state of the art would be in far better shape if we had tools as useful as NASTRAN for sizing computer systems.

Re: Danger of Sensitive Car Electronics

Will Martin -- AMXAL-RI <wmartin@ALMSA-1.ARPA>
Mon, 22 Aug 88 16:13:59 CDT

Interesting that this topic should be brought up just now. I just received in the mail a catalog on "Electrical Noise and Interference Control Courses, Publications, & Services" from Interference Control Technologies (Star Route 625, PO Box D, Gainesville, VA, 22065 (703)347-0030), which has on its cover a rather strange painting of a car going through a guardrail and over a cliff as the result of a radio transmitter radiating above a mountain tunnel opening. I say "strange" because the angle of the car and the tire tracks look unnatural, but then I'm no traffic-accident specialist.

Anyway, those interested in this topic may want to write for this catalog (it is the "September-February" issue) -- the company holds seminars and puts out books and symposium proceedings on the topic of EMC and EMI.

There's also a free controlled-circulation magazine on the subject; write to EMC Technology, Circulation Dept, PO Box D, Gainesville, VA 22065 Note the similarity to the above address -- I guess they are all part of the same organization.

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 40

Thursday 25 August 1988

Contents

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

Car engines become target for hackers (RISKS-7.39)

Jerome H. Saltzer <Saltzer@ATHENA.MIT.EDU>
Wed, 24 Aug 88 18:23:33 EDT

> False instructions will be detected and the owner told the change has
> invalidated the guarantee.

That approach has an interesting implication. It seems to mean that in order

to do a new microcode release the manufacturer will have to make sure that every service agency gets that release before any cars using the new release roll off the production line. In the past, delay in getting the latest update to a service agency would simply mean that the service agency didn't have enough information to do certain kinds of service on your new car. Now, it may mean that they will challenge your warranty. I wonder if the high-level executives who thought up that idea have checked it through with the people who do microcode releases.

Jerry

Re: IL car emissions testing process and enforcement errors

Will Martin -- AMXAL-RI <wmartin@ALMSA-1.ARPA>
Thu, 25 Aug 88 9:52:38 CDT

When I first heard of this, it did seem a poorly-designed system. It relates a variable which could be greater than 1, the number of cars a person may own, with a single item -- the owner's driver's license. Suppose you own three cars. One of them fails the test, and you may decide to stop driving that one for a while before getting it fixed. Meanwhile, you drive the other(s), which passed the test. The law would STILL suspend your driver's license due to that one car's failure. How do they handle cars being restored or otherwise in a perpetual state of disrepair, anyway? The emissions-test failure should be related to the specific vehicle, not to the owner. (What about cars that are owned by corporations or otherwise not tied to an individual, also?)

Again, there is an obvious way around this. The registered owners of private cars in IL should be non-drivers. Put your car(s) in your child's name, or in the name of your dog or a made-up name at your address. Then, the emissions test failures would relate to a name which did not match any driver's license, so the driver would not have his/her license suspended no matter the result of the test. As long as the taxes on the car are paid, and the license plates and/or stickers bought, it is still perfectly legal. I can see there being a bit of extra effort when you sell the car, as you would have to transfer ownership back to yourself before the sale took place, but that could probably be done with a single notarized document.

When 30% or so of the computer-matches for owners of cars that failed the tests come back with "no license on record", I guarantee the badly-designed law will be changed! (Of course, no guarantee that it will be replaced with anything better, given the history of incompetence in legislation through the ages... :-) At least the people can strike back at the system for a while, using this tactic.

Will Martin

---

re: Danger of Sensitive Car Electronics

Henry Schaffer <hes@uncecs.edu>
Thu, 25 Aug 88 09:31:36 edt

Will Martin <wmartin@ALMSA-1.ARPA> mentioned a catalog "Electrical

Noise and Interference Control" with a cover picture of a car going through a guard rail on a cliff. The heading by the car is "ANOTHER EMI INCIDENT?". This is certainly a dramatic and provocative picture. The "About the Cover" explanation in the catalog (quoted below) is interesting both for what it says and for what it implies:

"The installation of microprocessors for controlling critical automotive functions (engine control, braking, acceleration) has dramatically increased the modern vehicle's vulnerability to interference. Even the malfunction of non-critical functions (power sun roofs and windows, hood and trunk releases) has caused property damage, injury and even death.

"Although automotive travel has become safer, there are a growing number of complaints related to "unintended' acceleration as recorded by the National Highway Traffic Safety Administration. Dr. Roger L. McCarthy, P.E., of Failure Analysis Associates expects the trend to increase since the "overwhelming majority of vehicles produced since 1981 have had computer-controled engines." Complaints of braking system failure, sometimes simultaneous with unintended acceleration, and the inability to confirm the validity of these complaints in subsequent tests make the problem difficult to investigate or substantiate. Dr. McCarthy asserts, however, that "it would be equally erroneous to dismiss all such complaints as untrue. The problems associated with detecting and reproducing all types of transient electrical phenomena are well known, and phenomena such as single event upsets, where a transient electromagnetic disturbance changes the system state, only complicate things further."

"The detection and measurement of, design against, and retrofit to prevent electromagnetic interference is a science and a necessary developmental phase of any successful product -- commercial, industrial or military. This catalog is your guide to the latest in theory application and pragmatic approaches to the control of electrical noise interference.

--henry schaffer n c state univ

Automobile computer modifications (Re: RISKS-7.39)

<att!homxb!twitch!grt@ucbvax.Berkeley.EDU>
Thu, 25 Aug 88 07:25:04 PDT

Virtually all issues of Porsche Panorama have ads for ROM modifications for Porsches. They usually claim some number or percentage increase of horsepower, and they frequently contain disclaimers or warnings in small print, especially with respect to street legality in California.
I drive at race tracks, but I don't know if people are using modified ROMs. There are certainly some rather hot cars around. The 944 has a switch that tells the computer when full throttle is applied. Someone told me that I could get more power if I disconnected that switch. A more ordinary situation is drivability problems when the computer malfunctions. Sometimes I wish my car had a logic analyzer so I could figure out what is happening.

The computer costs $1400, so I do not want to carry a spare one just to avoid getting stranded somewhere.

George Tomasevich, att!twitch!grt AT&T Bell Laboratories, Holmdel, NJ

Statistical reliability estimation criticized (COMPASS '88 report)

Jon Jacky <jon@june.cs.washington.edu>
Wed, 24 Aug 88 16:34:21 PDT

> (Henry Spencer writes) ... there is no limit to the money that can be
> spent adding 9's to the end of 99.9999% reliability.

An important question asks whether those extra 9's are meaningful at all. One sometimes hears statements like, "for safety critical systems the probability of failure should be less than 10 ** -9" (ten to the minus nine power, or one in a billion). One even hears claims that the probability of failure of some system _actually is_ less than 10 ** -9 per hour. Is it meaningful to make such requirements for computer systems, or to claim that such a requirement has been met? The apparent consensus at COMPASS '88 (a meeting devoted to the safety and security aspects of computer systems held last June) was no, it is not.

Sal Bavuso of NASA-Langley Research Center recalled that the 10 ** -9 figure was derived from historical accident data for airframe failures: the probability of things like wings breaking off was observed to be about 10 ** -8 per hour of flight, so it seemed reasonable to require that control system failures not add significantly to the risk. Mike DeWalt of the Federal Aviation Administration pointed out that that 10 ** -9 figure was meant to apply to things that break or wear out, where it is reasonable to expect failures to appear randomly. He explained it was never intended to apply to design errors, which are what software errors are. John Cullyer of the British Royal Signals and Radar Establishment also said that the 10 ** -9 figure was meaningful when applied to analog computers composed of operational amplifiers, which are used in some autolander systems, but is not applicable to digital systems.

Douglas R. Miller gave a talk titled, "The Role of Statistical Methods in Software Safety Assurance" (it does not appear in the COMPASS proceedings but is available from the author at George Washington University). To explain his rather negative view of claims of very low failure probabilites, he postulated a system in which the probability of failing a test was random and was distributed in a Poisson fashion. He did a simple derivation to determine how many consecutive failure-free tests would be needed to establish with 99 percent confidence that the failure probability was less than some number. For example, how many successful tests must be run to establish with 99 percent confidence that the probabilitiy of failure is less than 1 in a billion? Common sense suggests that it must be at least a billion, perhaps more. Miller derived that you actually need around 4.61 billlion, and presented the rule of thumb that to obtain confidence that the probability of failure is less than 10 ** --N, you need about 10 ** +(N + 0.5) trials. He pointed out that in most cases it is only practical to test up to around 10 ** 5 trials, which can only reveal

bugs that appear with frequency 10 ** -4.5 or greater.

Miller said that people sometimes say that good engineering practices ensure that the probability of failure is much less than 10 ** -4.5. But, he said,
this is rather illogical if testing reveals any errors at all. If the tests
reveal frequent bugs, why should you believe that your good engineering
practices have prevented the subtle ones?

Cullyer said, "Let's throw out the 10 ** -9" - and many of the audience
responded with enthusiastic applause. Someone asked if he would accept a
failure probability of only 10 ** -4 or 10 ** -5 for nuclear weapons safety.
He responded, "In the weapons area there should be no room for probability. If
something is unthinkable, don't let it happen. You either certify it or you
don't - one or zero."

Nevertheless, statistical claims are very ingrained among some systems safety
practitioners. Nancy Leveson of the University of California at Irvine
recalled a conversation with an engineer who kept pointing to a box on fault
tree labelled, "software failure." He wanted to know what number to fill in
for that probability of that event. Leveson tried to explain that there was no
meaningful number, but he persisted. Finally she answered, "Just write 1.0."

(This is an excerpt from a report on COMPASS '88 that will appear in the
October issue of ACM SOFTWARE ENGINEERING NOTES).

- - Jonathan Jacky, University of Washington

Can current CAD/simulation methods handle long-term fatigue analysis?

Gerry Kokodyniak <kokody2%me.toronto.edu@RELAY.CS.NET>
Thu, 25 Aug 88 13:35:47 EDT

Henry Spencer <henry@zoo.toronto.edu> in RISKS DIGEST 7.38 states:
As I understand it, metal fatigue in general is poorly understood, and there
is really no way of calculating it.

Metal fatigue can be calculated with a reasonable amount of accuracy.

..... The whole area is still very much
rule-of-thumb engineering plus empirical testing. There are rules that
give a rough idea of the fatigue life of an airframe, after which a big
safety margin is added (we're talking factor of 2, not 10%). Even this
is only a tentative number.

Most aircraft design use a 10% to 20% safety factor. A safety factor of
two would make an aircraft so heavy it would never leave the ground.
Adding a safety factor of two, without making a component bulkier would
mean a shift towards high strength alloys. As a general rule of thumb,
high strength alloys tend to be more brittle and therefore less damage
tolerant. These "high strength" alloys could catastrophically fail due
to microscopic sized cracks. A very bad feature in regards to inspection.

The problem is not so much that fatigue behaviour is not understood very well as that the actual loading conditions can never be acurately modeled. An example is a turbulent flight vs. a smooth flight; poor engine maintenance; airlines allowing luggage past the allowed weight limits; rough landings by "rough" pilots. There are many factors that influence the actual loading conditions. Because the load cannot be modeled accurately, any technique i.e. F.E.M to just using a stress formula will be out. Regular inspections are meant to catch cracks (caused from abnormal/normal loads before they have a chance to propagate to dangerous sizes i.e. the critical crack length).

Without Computer Aided Engineering / Finite Element Methods, the space shuttle would never have flown at all. The FEM was used in applications from modeling fluid dynamic flow over the shuttle to stress analysis to thermal modeling. FEM can be used in coordination with fracture mechanics models to model cracks and to determine the damage tolerance of the component being modeled.

Last point, CAE & FEM can be very powerful tools when coordinated with Fracture Mechanics data obtained from experiments. There are many FEM codes that allow one to enter such data and have elements that model cracks and crack propagation very well. These can be powerful tools if used properly.

Gerry Kokodyniak

Gerry Kokodyniak, Ph.D. Student, Dept of Mechanical Engineering, U. of Toronto
USENET: kokody2@me.toronto.edu Structural Integrity Fatigue and
BITNET: kokody2@ME.UTORONTO Fracture Research Laboratory
UUCP: {linus,allegra,decvax,floyd}!utcsri!me!kokody2 (416) 978-6853

Boundary Cases

James Peterson <peterson%sw.MCC.COM@MCC.COM>
Tue, 23 Aug 88 17:37:33 CDT

Vol 7, Issue 38 contained two articles that are more related than they might seem: Tom Lane mentioned a problem with a water billing system that ignored the wrap-around case of a meter that went from 998 to 2 and David Sherman mentioned a Florida couple that got a $5,062,599.57 electric bill.

The wrap-around problem is when a current meter reading is less than the previous one. In Tom's case it was because of the limited number of digits on the meter. His system was programmed to ignore it, possibly as an assumed input error. "Obviously" in this case, it should have been wrap around.

A few years ago, however, my meter was replaced. The reading one month was 0456 and the next month it was 0002. The billing program assumed it was wrap around and charged me for 9546 units -- about 2000 times my normal usage. Last month, however I had an actual misreading -- the previous reading was 0680 and the current reading was 0660 (the 0680 we suspect should have been 0630). Service has improved however, because they caught that one somehow and simply sent me a corrected bill with a credit for the misbilling.

The problem is how to identify a wrap-around as different from a misreading or a new meter. The only solution I can figure is to keep a history on-line of what the recent periodic bills have been. When new bills are calculated, the new bill is compared with the on-line history. Bills which are way out of line (like the Florida case) can be easily caught that way. This is a simple sanity check and seems to be basically what people do.

Does anyone know if this scheme is used in periodic billings (like utilities or charge cards?).

There can admittedly be problems -- during start-up there is no past history to work from (at one job, the operator entered my yearly salary as a monthly salary and my first paycheck was $12,000) and sometimes things simply change (like the change in a credit card usage for the yearly vacation), but it would seem to be a valuable way to catch a lot of the outlandish billing problems that you see blamed on computers.

jim

Re: Another boundary case bug

John Bruner <nlp3!jdb@mordor.s1.gov>
Thu, 25 Aug 88 15:42:45 PDT

Tom Lane's problem with his water meter calls to mind a problem I had about a year ago with mine. My new home had a brand-new water meter with a digital (odometer-style) readout. The water bill for my first month was over $400.

When I checked my meter it appeared to me that the meter reader had misread it by a factor of ten. I called the water company. They said yes, the bill did seem high, but they sent someone else out to double-check it and I really was using that much water. The water consumption on my bill was given in units of CCF. I asked if this represented 100 cubic feet. They didn't know. (Recently I noticed that they've added an line to the bill that does indeed define CCF as 100 cubic feet, or about 750 gallons.) I could not reason with them about this -- their attitude was that I clearly did not know what I was talking about (!).

Finally I convinced them to send someone around to look at it with me present. With the company representative watching the meter I flushed a toilet. By my calculations the toilet consumed 4 gallons. By theirs it consumed 40. I pointed out that the meter was clearly labelled CUBIC FEET, that it read in units of 1 cubic foot, and that to read it they needed to discard the last two digits.

Finally I found out the problem: the older digital meters read 10's of cubic feet, and the 10's digit was white-on-black, so all the meter reader had to do was copy down the digits that were black-on-white. In my case, though, because he didn't know what the billing units were, he couldn't convert cubic feet to CCF. All of the digits on my meter were black-on-white, so he just guessed. A considerable effort

on my part was required to undo the effects of his guess.

The solution to my problem: the water company replaced the meter with one of the older ones.

John D. Bruner Natural Language Incorporated
nlp3!jdb 1786 Fifth Street, Berkeley CA 94710 (415) 841-3500

Mother's maiden name == arbitrary password

Walter Smith <wrs@apple.com>
Wed, 24 Aug 88 20:14:23 PDT

Institutions have used "your mother's maiden name" as a password for years. The wonderful thing is that you can *lie* with no ill effects. When you see "Mother's maiden name" on a form, think of it as "Password (must be a last name)".

[This was also noted by several other contributors. PGN]

The really frightening "factoid" coming into common use is the last N digits of your social security number. I've seen two or three touch-tone operated banking systems that use it. One of them even said something like "Your account is secure from unauthorized access, because your personal code number must be entered first. The code is the last four digits of your social security number."

- Walt
Apple Computer Inc., 20525 Mariani Ave. MS 46-A, Cupertino CA 95014

Risks of EFT agreements

Doug Claar <dclaar%hpda@sde.hp.com>
Thu, 25 Aug 88 12:49:00 pdt

I recently received an application to sign up for our Credit Union's phone-based electronic funds transfer system. The application required three items: my account number, my self-assigned PIN, and my signature agreeing to be responsible for any transactions completed with my PIN! To make matters worse, the application itself is a fold-in-half and mail thing, with pre-paid postage on one part of the outside, and big advertisements of what is inside on the other side. Finally, by signing the agreement, you agree to be governed by the Credit Union's rules regarding EFT, which you are not given, but which will be sent later. So many risks from one little application...

Doug Claar, HP Information Software Division
UUCP: { ihnp4 | mcvax!decvax }!hplabs!hpda!dclaar -or- ucbvax!hpda!dclaar
ARPA: dclaar%hpda@hplabs.HP.COM

Chile con backbones

Martin Minow THUNDR::MINOW ML3-5/U26 223-9922 <minow%thundr.DEC@decwrl.dec.com>
24 Aug 88 14:25

Anyone who has been running with the University of Chile as their closest backbone server may have noticed bizarre things lately. There were some problems; the newest node list changes the weights of the link to try to keep North American mail from going to South America first (and getting delayed).
--- Joe M.

An item by Mark Garvin on Softguard and the Trojan horse "SUG"

<Neumann@csl.sri.com>
Thursday, 25 Aug 88 18:00:05 PDT

A rather extraordinary message from ZDABADE%VAX1.CC.LEHIGH.EDU@CUNYVM.CUNY.EDU appeared on VIRUS-L, describing Trojan horses (often named "SUG") that have been promoted as SoftGuard/SuperLock UNPROTECTORS (lock-breakers). The file is rather long (about the size of a typical RISKS issue) and of particular interest to those concerned with Trojan horses and legal implications. The full text can be FTPed from KL.SRI.COM stripe:<risks>risks-7.40softguard. PGN]

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 41

Wednesday 31 August 1988

Contents

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

The Marconi Deaths

Brian Randell <Brian_Randell%newcastle.ac.uk@NSS.Cs.Ucl.AC.UK>
Wed, 31 Aug 88 10:57:28 WET DST

Last week a further Marconi employeee died in somewhat mysterious circumstances. I did not see any original press reports, but only the attached editorial from the Independent. The Independent is not a sensationalist tabloid, but rather a highly respected and respectable national newspaper here, so the fact that it chose to devote its leading editorial to the Marconi issue is of some note. The result provides what I would regard as a balanced summary and commentary, which I therefore thought was worthy of passing onto the RISKS readership, given the previous coverage of these matters in RISKS.

Brian Randell, Computing Laboratory, University of Newcastle upon Tyne

[For those of you wishing to comment on the relevance of this topic, the plausibility of conspiracy theories, the credibility of the debunkers, etc., please first dig up the back issues on this topic, namely RISKS-4.74, 81, 83. And let's keep the speculation down on this one. On the other hand, if there is any DEFINITIVE knowledge, let's hear it. PGN]

DEATHS WHICH MUST BE INVESTIGATED

The Independent, Friday 26 August 1988

(Reprinted in full, without permission)

The police said it was suicide, and no doubt they were right. Ex-Brigadier Peter Ferry, a marketing manager at Marconi's Command and Control Systems centre at Frimley, Surrey, had apparently killed himself by inserting mains electric wires into his mouth and then turning on the power. The method chosen was perhaps marginally more grisly than in the case of several other Marconi employees. In 1986, for example, Ashad Sharif, a computer analyst who worked for Marconi Defence Systems in Stanmore, Middlesex, tied one end of a rope around his neck, another to a tree, and put his car into gear. Two months earlier, the body of Vimal Dajibhai, a software engineer responsible for checking the guidance systems of Tigerfish torpedos for Marconi Underwater Systems, was found under Clifton suspension bridge at Bristol. In March 1987, David Sands, a project manager working on secret satellite radar at Marconi's sister company Easams, in Camberley, drove up a slip road on his way to work and into a cafe at an estimated 80mph. A year later Trevor Knight, a computer engineer at Marconi's space and defence base in Stanmore, died in his fume-filled car at his home in Hertfordshire. Earlier, two other Marconi employees, Victor Moore, a design engineer, and Roger Hill, a draughtsman, had killed themselves, both seemingly
as a result of work pressures.

There have been at least half a dozen more untoward deaths among defence scientists and others working in the defence field. Marconi is not alone, but it is well in the lead. The best efforts of investigative journalists have failed to establish a link either between the various deaths or between the deaths of the Marconi staff and the Ministry of Defence inquiry, now two years old, into some (pounds)3bn worth of defence contracts awarded to GEC-Marconi. No doubt in several instances pressure of work was the main factor: in a field where millions of pounds hang on the securing of contracts, it can be intense, especially if the Ministry of Defence investigators are hovering, as they had been at Frimley, Brigadier Ferry's base. It is hard to believe, however, that other factors have not also been at work. The pressure of work is also fierce in the money markets of the City, where equally large sums are at stake. Yet the suicide rate remains unremarkable.

Mr Ferry's death on Tuesday must add to the concern already aroused by the alarming sequence of deaths in the defence industry. He had apparently been depressed since his car collided with a lorry a month ago; but suicide seems an extreme reaction. In such instances where no foul play is suspected, the inquiries of both police and coroners are likely to be brief, partly for the

sake of the distressed relatives. They will not be concerned with establishing a connection with comparable deaths in different counties. Since these cases have been spread wide, there is now a case for pulling the threads together. It may be that there is no conspiracy and no concerted skullduggery. But these have been talented men. To allay anxieties, a senior police officer should be appointed to head a coordinated investigation into the underlying causes of so high a death rate.

$300,000 Automatic Teller Theft (Sort Of)

Henry Cox <cox%spock.ee.mcgill.ca@Larry.McRCIM.McGill.EDU>
Wed, 31 Aug 88 14:30:32 edt

THEFTS FORM AUTOMATIC TELLERS WON'T HURT CLIENTS: DESGARDINS
(From the Montreal Gazette, Monday 29 August, 1988)

Desjardins credit union customers are being told not to worry about the theft this year of $300,000 from automatic tellers. [What, me worry?]

Bruno Morin, Desjardins senior vice-president in charge of administration, said the money disappeared from three locations between February and June. Morin assured automatic teller customers that their transactions won't be affected by the unsolved crime, believed to be "an inside job". The amounts stolen are guaranteed by insurers. He added that some changes have been implemented which should avoid any similar thefts. Morin dismissed reports that the $300,000 was stolen by thieves who tampered with the credit union's computer information system. "The computer had nothing to do with it. People got in and stole the reserves. It's pure and simple."

What isn't so simple is finding out who took the money. We know exactly the hour and minute the money was stolen and where it was stolen from - just not who did it,", he added. Although Morin wouldn't divulge which automatic tellers were hit, he didsay non was on the island of Montreal. One was in Longueuil [a suburb on the South Shore], he said.

Francois Aubin, a public affairs vice-president of Desjardins, said the money appears to have been taken when the machines were being loaded. The automatic tellers are supplied by money by Desjardins employees as well as Secur, an affiliated security company.

Car engines become target for hackers (RISKS-7.39)

Jeffrey Mogul <mogul@decwrl.dec.com>
26 Aug 1988 1313-PDT (Friday)

In RISKS-7.40, Jerry Saltzer worries that if auto repair places must verify the microcode in a car computer, that there will be problems with out-of-date service information; a service agency that hadn't yet received (or had already discarded) the microcode for YOUR car might challenge your warranty.

This seems like an obvious application of digital signatures: dedicate some portion of the ROM to a value derived from an encryption of the rest of the ROM (plus some standard validation pattern). ROM hackers without the encryption key could not generate a valid ROM signature.

Key security is clearly problematic; it would be greatly simplified if a public-key system is used, so that rather than requiring key security at ever repair shop, the key need be known only when the ROM code is compiled at the manufacturer. Since it doesn't matter how long the crypto function takes to compute, any sound public-key system could be used (perhaps avoiding large license fees).

10 years ago, Jerry wrote an article for Operating Systems Review pointing out some problems with digital signatures; but since nobody is going to try to disclaim one of these ROM signatures, the problems he raised then do not apply here.

-Jeff

Blinker failure in 87 Ford Mustang

<thomas@xenurus.gould.com>
Wed, 31 Aug 88 17:59:09 CDT

Reading the discussion of car acceleration problems in RISKS has prompted me to write of a personal experience I have had with my 1987 Ford Mustang. I was on a trip to Kentucky about 6 months ago, and while in one of the towns had an interesting problem. I suddenly noticed that, although I was using the turn signal arm appropriately for all of my actions, the turn signals did not seem to be activated on the dashboard. I quickly turned down a side street, put the car in park (but didn't turn the engine off), and had a friend of mine who was with me get out and check the turn signals. Sure enough, they were *not* being activated!

Being of the experimental sort, I then proceeded to put on the emergency flashers, which worked correctly. I shut them off and once again tried the turn signals. Low and behold (you guessed it), the turn signals worked fine! What went through my mind at that point was, what if I had been in an accident and someone accused me of not properly signaling? What could I say in my defense? Would anyone believe me?

I did not report this to the dealership since I considered it an intermittent computer problem that they would probably *never* find. Also, the problem has never reoccurred (to my knowledge). The problem may not be computer related, but it sure sounds like it is!

Tim Thomas, Gould CSD Urbana, Urbana, IL 61801
(217) 384-8718 uucp: ihnp4!uiucuxc!ccvaxa!thomas

Risks of locking systems

Andrew Birner <Andrew-Birner%ZENITH.CP6%LADC@BCO-MULTICS.ARPA>
Sat, 27 Aug 88 12:37 PDT

In Risks 7.37, Leonard N. Foner (foner@wheaties.ai.mit.edu) writes:

> Whatever happened to good, old-fashioned mechanical locks?

Not even a simple mechanical lock can protect you when the locking system is poorly designed. The scheme installed in our computer room a few years back illustrates this:

The computer room is acessible from two sides. On one side is a simple double door (for bringing in supplies, etc.), secured with a basic jimmy-proof cylinder lock. Maintenance has a key to this, so that they can get in to check the air conditioning filters and water lines. On the other side, we installed a vestibule with output bins, to protect our operators from chatty users.

The door from the vestibule to the computer room has a mechanical combination lock; you punch in some numbers and turn the knob, and the door (usually) opens. From inside the computer room, the door is opened by simply turning a crank. Clearly, if you don't know the combination, you can get from the computer room to the vestibule, but not back in again.

After we installed the vestibule, we replaced the old door to the corridor. We changed the direction of swing, and also got rid of the door knob, so that users could just push it open. Of course, we still wanted to lock the vestibule during off hours, so we asked maintenance to install a deadbolt, which they cheerfully did. This deadbolt was actuated by a key on the outside (corridor side), and had NO ACTUATOR AT ALL on the vestibule side!

This arrangement made it perfectly possible for someone to get trapped in the vestibule, with NO WAY OUT! I complained of this, but nothing came of it; maintenance apparently decided the probability was low enough that they needn't worry. I doubt the fire inspector would have been impressed, but this didn't seem to bother anyone.

About a year after this was installed, a maintenance engineer entered the room via the back entrance, to clean the AC water filters. After filling a bucket with water, he decided to go out the front way, since it was closer to where he wanted to dump this water. He went into the vestibule, letting the door latch behind him, and tried to open the corridor door--which was, of course, locked! Naturally, he didn't know the combination (why should he? He had a key, after all...), so he was quite effectively trapped.

Since he didn't feel like waiting until the watchman came by, our hero kicked his way out through our output bins, doing a fair amount of damage. There is now an actuator for the deadbolt on the inside of the vestibule...

Andrew Birner

Electronic 1040s

Rodney Hoffman <Hoffman.es@Xerox.COM>
31 Aug 88 12:24:39 PDT (Wednesday)

From the August 31, 1988 'Wall Street Journal':

Electronic filing [of tax returns] advanced despite computer software

snags, says the General Accounting Office. Such filing of computer-ready returns by preparers speeds processing and refunds and slashes errors. The IRS plans to expand it to 48 districts in 1989 and to all 63 in 1990; volume could reach 35 million returns in 1993. Congress's General Accounting Office reports that IRS successes in handling about 580,000 such returns from 16 districts this year came despite glitches that prompted the IRS to make many software corrections without the required testing of effects.

As a result, the IRS is waiting for final corrections before going back to make permanent electronic records of the returns. Now it is examining ways to eliminate the need to submit signatures and W-2 tax-withholding forms separately on paper. And it will work to recruit smaller return preparers for 1989; this year, H&R Block offices filed 82% of all the electronic returns....

The IRS's Greensboro district, covering North Carolina, this year produced 123,386 electronic returns -- over 21% of all such filings. The Dallas district ranked second with 70,832 returns, or over 12%.

---

water seepage stops Computer controlled monorail

George Michaelson <munnari!ditmela.oz.au!G.Michaelson@uunet.UU.NET>
Thu, 01 Sep 88 10:29:15 +1000

Details in "COMPUTING australia" of Aug 29

Water seepage into Sydney's new monorail PLC (Programmable Logic Controller) halted the system. the GEC-Digital 140 PLC which is located in the nose of the train has been tested with an HP analyser to try and simulate the fault.

The monorail is highly automated. One breakdown had dozens of passengers stuck in a sealed environment for over 2 hours, with complaints about heat & lack of fresh air. Many people resent the monorail as a pointless and expensive intrusion into the city, but there have also been fears voiced about the safety of automated systems like this.

Re: Fewer Charges Now Require a Signature

attcan!lsuc!dave@uunet.UU.NET <David Sherman>
Sun, 28 Aug 88 23:09:58 EDT

Petro-Canada, the government-owned oil company that competes on the market here with the rest of the biggies, switched to a "no signature" system a few months ago. You get your card back along with what looks like a normal cash-register receipt. It has a line for signing on it, but you only get one copy and the attendant tells you that's all there is.

The first time this happened to me, I did a doubletake, thought a second and decided that if they didn't WANT my signature, I wasn't going to complain. A couple of months later an article in the Toronto Star noted that Petro-Canada

will change this policy, due to customer complaints (people somehow think that not signing a credit card slip makes them more liable to false charges). Last time I was at a Petro-Canada, they were still doing it, though.

Continental Bank Drops Retail Accounts

<sun!portal!cup.portal.com!Patrick_A_Townson@unix.SRI.COM>
Sun Aug 28 11:06:22 1988

[PATRICK: Sorry, mail to you fails, thus no earlier responses. PGN]

On August 15, 1988, Continental Illinois National Bank of Chicago discontinued retail banking operations. All retail checking and savings accounts on that day were transferred intact to the First National Bank of Chicago.

Most readers will recall that during 1984, Continental went belly-up. Unlike many other banks which have collapsed, Continental was given a huge infusion of money by the feds and kept afloat. Over the three years which followed, Continental again squandered alot of its money, leading the feds to demand some radical changes in one of the largest banks in the world, and the largest bank in Chicago.

One of these changes was to get rid of all non-profitable banking business, which was defined to include retail accounts, or the accounts of little folks like you and I. Many of us with Continental accounts in the dark days of 1984 stuck it out without batting an eye. This time around, we were given no choice in the matter of our bank loyalties.

The switch to First National Bank was announced several months ago. The change became effective on Monday, August 15. *No action of any sort was required of customers.* We did not have to do a thing. Beginning about August 5, FNB began mailing out new ATM cards and PINS. Several days later, they began mailing out new checks. About 40,000 customers of Continental were involved, so there were some errors in getting the new checks and ATM cards out to the proper address, but these are now largely resolved.

We were told to begin using our new checks from FNB on Friday, August 12, under the assumption these checks would not reach clearing until at least August 15. We had to discontinue the use of the Continental ATM cards on Friday, August 12 at 2:00 PM, and were allowed to begin using the cards from FNB as of Monday, August 15 at 8:00 AM. Our only real inconvenience was the inability to use Cash Station machines over that weekend. Continental will continue to manually clear checks written before August 15 which come through for the next two months. They will be forwarded to FNB to be charged on our accounts. Continental issued a final statement on August 15, and waived the usual service charges for the final month. For about ninety percent of the old Continental customers, they will have the same closing date on their statements from First National Bank.

As an added courtesy, FNB *will not have service charges of any kind* on these accounts transferred from Continental for one year, until 9-89. The first

batch of 300 checks on the new account are free. There will be no ATM fees. There will be no per-check or monthly fees. Since the accounts were not considered 'new accounts' under federal regulations, the new supply of checks for each customer began numbering at 1001 instead of 101 as on new accounts, and the original date of opening was omitted from the face of the check.

FNB also took over the branch bank facility Continental had operated at 1150 North Clark Street on the corner of Division Street, and will continue to operate it as a branch bank. Since both banks belong locally to the Cash Station network, there is no difference in the location of ATM's in the area. Continental belonged nationally to the PLUS network, and FNB is in the CIRRUS network, so there will be some differences when travelling outside the Chicago area, but these should be minimal.

On Monday, August 15, the teller lines at FNB were *much longer* than usual, as large numbers of former Continental customers qued up to make sure their money had actually been transferred without a hitch. Of course those of us ATM devotees who wanted to check merely had to go to any machine and inquire, to make sure everything was okay.

People who had not received their new check stock and ATM cards as of August 15 were issued temporary checks on the spot in the bank, and ATM cards were printed on an embossing machine nearby. Perhaps several hundred out of the 40,000 customers transferred had failed to receive either their new checks, their ATM card or their PIN by the cutover date, but overall, the transition was quite smooth. Employees were stationed in the lobby at Continental for about two weeks before and after the change, handing out information on the transfer. One customer service representative will continue to be on duty in the lobby of Continental for about another month.

Although I did have a fight with FNB about fifteen years ago which obliged me to sue them (I won the matter!), I have decided I will try them again for awhile, especially since the account is free of all charges for the next year. I might add the checkstock is more attractive also. My new account has a picture of the Chicago skyline on the check.

My pay-by-telephone account was also automatically switched over. We have here in the Chicago area a system by which the utilities (gas, phone and electric) can be paid through a simple phone call to a central computer, and I was concerned at first if this would be changed also. It was, so far as I know, with no hitches whatsoever.

The cash machines are responding a little differently though. Under the old Continental account the machines would accept 'split deposits', that is, you could deposit a check and take cash back from the deposit. Under the new account with FNB -- even though its the same Cash Station network -- you have to make two transactions: one to deposit the check, the other to withdraw the desired cash. Likewise, under Continental, you could not get your balance on line until about two months ago. FNB says they have always offered that to their customers. At Continental, we could ask the machine to give us the time, date, and nature of the last transaction; FNB says they are unable to do this. Etcetera...small minor differences, but overall a very smooth conversion of accounts.

Continental's credit card portfolio was sold about a year ago to First National, so VISA and MASTERCHARGE cards from that bank have already been getting processed for several months by the FNB card center in Elgin, IL. About 2000-3000 Continental customers decided not to make the switch, and sought out new banking arrangements of their own during the summer.

Patrick Townson

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 42

Thursday 1 September 1988

Contents

- "Pizzamation" traces phone calls, matches addresses
  Jon Jacky
- Skylab and Sunspot Activity
  PGN
- Denial of Service in Wembley-on-the-Motown
  Behrooz Parhami
- Re: Calculations with wrapped numbers
  Mike Linnig
- Meter reading follies
  Chris Jones
- Re: abnormal bills
  Ted Lee
- Risks of CAD programs
  Mike A. Gigante
- Re: Risks of CAD programs
  Sam Crowley
- Can current CAD/simulation methods handle long-term fatigue analysis?
  Henry Spencer
- Re: Vincennes and Non-Computer Verification
  Henry Spencer
- Re: Computers and Gambling
  Jim Frost
- Automatic Bank Procedures
  David A. Honig
- Info on RISKS (comp.risks)

"Pizzamation" traces phone calls, matches addresses

Jon Jacky <jon@june.cs.washington.edu>
Thu, 01 Sep 88 09:10:40 PDT

Excerpted from a story in THE SEATTLE POST-INTELLIGENCER,
18 August 1988, pps. B5 and B8:

CHAINS ARE PUTTING THE BYTE ON PIZZA DELIVERIES by Jim Erickson

Tim Turnpaugh was caught off guard recently when he telephoned for a pizza to be delivered to his home. When he got the pizza company on the line, the person taking orders greeted him by name like an old friend -- before Turnpaugh could identify himself -- and cheerily asked if he'd like the same toppings he asked for on a previous order.

"I didn't have to give them directions to my house, nothing," he said. Everything the company needed to know was gathered during a previous purchase and stored in the memory of a computer, ready for instant regurgitation. This is the brave new world of pizzamation.

Godfather's pizza in Washington [state] is one such firm on the cutting edge of pizza technology. Inside a gray-walled, nondescript building in a Renton [Seattle suburb] business park, 80 desktop computers are lined up in rows at Godfather's state communications center. Not a single pizza oven is in sight. On a hectic Friday night, as many as 50 part-time employees sit in front of the tricolor screens, taking orders. ... If you've called before, the computer instantly identifies and recognizes your telephone number, and retrieves information from previous orders. "Customers don't even know a lot of the time they've reached a centralized system," said Donna Brown, manager of the center. "They still think they're calling a local restaurant." ...

After the order is placed, the computer decides which of 51 restaurants or outlets in Western Washington, or 10 in Eastern Washington, is closest to the customer. The computer totals the price and relays the order and delivery instructions to the kitchen of a restaurant or outlet, where it comes out on a network printer. ...

Brown said the system allows the company to keep track of sales data, and since it records addresses -- more than 500,000 are stored in Godfather's memory banks -- it can be used for direct-mail marketing. ...

Cathy Nichols, owner of four franchised Domino's Pizza stores in Renton and Maple Valley, installed computers early this year ... Since the computer matches phone numbers with addresses, it also helps smoke out young pranksters who habitually order unwanted pizzas for the unsuspecting. ...

[Not if they are smart enough to read a phone book. PGN]

Some customers may worry that their local pizza retailer may be keeping records on their eating habits as well as detailed directions to their house. It can be unsettling to think that the Big Cheese is watching you. Nichols acknowledged that large, centralized systems are "kind of scary." "There's one number in the state that you call, and they know everything about you."

Bill Brown of Godfather's said she could recall only three people who asked that their records be purged, and only because they didn't want to wind up on mailing lists. Their records were immediately removed, she said, adding that Godfather's does not sell its mailing list to other companies.

[This is the first confirmed report I have seen of marketing outfits tracing calls, although I have heard rumors of other systems in which calling an 800-

number in response to some promotion would put your phone number on a list that would later be matched in order to derive your name and address. It is my observation that most people believe that "tracing a call" is still a difficult, time consuming process that cannot be done routinely. This story shows that it is a service phone companies offer to commercial customers, although I have not seen any reports of it also being offered to residential customers (who would then be able to ignore calls from marketers, cranks, etc.) Jonathan Jacky, University of Washington]

[In an unrelated development, some of the pizza outfitters are selling leather pizza outfits -- that is, protective clothing for the pizzas. If the pizza chains are going into leather, maybe S&M now stands for salami and mushrooms. PGN]

Skylab and Sunspot Activity

Peter Neumann <neumann@csl.sri.com>
Fri, 26 Aug 1988 14:30:16 PDT

There is an article by Richard A. Kerr entitled ``Heads Up! Sunspots Are Dragging Down Satellites'', Science, vol 241, 19 August 1988, p. 902. He discusses the ups and downs of sunspot activity, and recalls that the last time a relative maximum was reached in 1979, the 85-ton Skylab satellite was downed as a result of the increased drag from the sun-swollen atmosphere. The predictability of future activity is apparently very poor. Computer relevance? Well, just one more thing to remember next time you put a computer in space to control something, along with cosmic rays, laser beams, meteorites, space junk, and other assorted hazards.

Denial of Service in Wembley-on-the-Motown

Peter Neumann <neumann@csl.sri.com>
Wed, 31 Aug 1988 18:34:41 PDT

Stevie Wonder's birthday concert for Nelson Mandela at Wembley was disrupted when someone stole a portable digital audio tape machine and a computer disk drive that links into his Synclavier. After a three-hour delay during which he could not perform the intended program without the equipment, only two songs were sung and the synthesizer pieces were omitted completely. (The equipment was later found.) [From England's COMPUTING, 16 June 1988, p.3, contributed by Behrooz Parhami, Computer Science, Carleton University, Ottawa CANADA K1S 5B6]

[Here is another example of the risk of becoming completely dependent on technology -- no longer being able to function without it. On the other hand, the equipment is presumably so reliable that there is little incentive to provide much in the way of backup facilities?]

Calculations with wrapped numbers (RISKS-7.40)

<linnig@skvax1.csc.ti.com>
Mon, 29 Aug 88 16:19:22 CDT

James Peterson <peterson%sw.MCC.COM@MCC.COM> writes:
>The problem is how to identify a wrap-around as different from a misreading...

We had a similar problem with wrapped data on a missile guidance system. Every few milliseconds we would get a target position update. To smooth out the noise we'd average the new input with the old. Since target positions were in degrees from true north they ranged from -180 to + 180 degrees.

The problem occurs when the previous value is -175 or so and the new value is +175. What is the average? Adding and dividing by two doesn't cut it (zero is certainly NOT the answer).

I don't remember how we solved this particular problem, but I have thought about it since then. Imagine trying to compute the average position of the second hand on a clock. You sample the position once a second for sixty seconds. Ok, now what is the average?

Mike Linnig

---

meter reading follies

Chris Jones <ksr!clj@harvard.harvard.edu>
Fri, 26 Aug 88 15:42:34 EDT

About three years ago I had an extended interaction with our gas company (Boston Gas), because of an error which was allowed to override all other readings. Boston Gas replaced our meters as part of what they say is a program to replace the meters every seven years. (In fact, I notice that they have replaced the meters three times in the thirteen years we've owned the house, but it certainly doesn't bother me to have the gas company look at our service and say it looks non-explosive). The old meters were the boxes with which I was familiar; the new meters were smaller by about 50% in volume, and had digital readouts.

As is standard practice, which practice had, until then, been working smoothly, our old reading was sent in along with our new reading.

It took many months of ridiculous bills, and numerous (well, four) trips by the gas company to notice that we were being billed amazingly incorrectly. The things that went wrong were:

1. The initial reading was wrong (*THIS* was the uncorrectable mistake). I was *AT LAST* able to convince the gas company that all of our data made sense if they first assumed that the first meter reading had been made from right to left instead of left to right (this is a somewhat obvious mistake since non-digital meters should be read from right to left).

2. Since my wife and I were not at home during the normal working hours of Boston Gas's meter readers, we were sent estimated bills

for months (about 14, all told). It occurs to me that the price of the gas fluctuated during this time, and they have no way of knowing when we were using high-priced gas and when we were using low-priced gas. It probably didn't make more of a difference than writng them 10 letters did, which is what we, in fact, did.

3. MOST ANNOYINGLY, eventually our gas meter reading caught up to what BG thought made sense. So, they called us, since now their bills showed that instead of owing them about $1300, they had overcharged us by about $400. It *only now* had become a problem that they wanted to solve. It took me about 10 minutes on the phone to convince the service person that I understood what was going on. As a matter of fact, when they finally read our meter, and believed the reading, it turned out that they owed us $5, which I declined to accept, knowing that, in New England in the middle of winter, I had impending multi-hundred dollar heating bills and could wait several weeks to realize my $5 credit.

So, what had happened? One incorrect reading had been accepted as correct, and someone (or someone's algorithm) had summarily rejected all subsequent readings, even though an examination of them would have revealed that they were all consistent ****with the exception of the initial reading****!!!!

It works to be first, even if you're wrong.

Re: abnormal bills

<TMPLee@DOCKMASTER.ARPA>
Fri, 26 Aug 88 01:33 EDT

Yes, some periodic billers do notice abnormal bills. When I first installed a modem on my Apple (must have been about five years ago) our oldest son, then about seventh grade, used it to call the usual local bulletin boards. (By the way, they outgrow the habit -- neither of our two kids has bothered in the last several years.) On some of them there were posted the usual lists of bulletin boards all over the place, national and international. ("for neat stuff call 01144 ...") Somehow either we or the U.S. public education system had neglected to inform grade school students that any phone number over seven digits cost money, and real long numbers cost lots of money. Needless to say, the next month's phone bill was out of sight. (I vaguely remember it was about $300, when usually it was around $20 or so.) We almost immediately got a call from the phone company asking if there was some kind of error and whether the bill should be corrected. I'm afraid I didn't have the presence of mind to ask how they noticed it.

(And no, it wasn't a "small town" phenomenon: the Twin Cities metropolitan area is about 2 million people and incidentally has one of the geographically largest toll-free phone systems in the country.)

Ted Lee

Risks of CAD programs (RISKS-7.38)

Mike A. Gigante <munnari!cidam.rmit.oz.au!mg@uunet.UU.NET>
Sun, 28 Aug 88 09:22:52 EST

> Do practicing civil engineers reduce their safety margins these days because
> they use computer-aided analysis? How much? How small a safety margin ...
> Alan Kaminsky, School of Computer Science, Rochester Institute of Technology

In my previous life, I was an Aeronautical Structures Engineer specializing in CAD/FEM at an active design organization.

FEM isn't new, computers were being used in the 50's to do structural analysis (matrix methods on mainly truss structures), then and now, the programs are not a panacea for an indepth knowledge of both teh behaviour of structures and of how the program works. Any engineer using these methods without that understanding is both incompetent to do the design and dangerous. There are a million different ways to represent your structural model with a wide variation in the quality of the results, you need to know what you are doing and what simplifying assumptions have been made in the element formulation!

Luckily, there are a number of checks in the engineering design process. there are regulatory authorities who need to independently varify the design (at least for aeronautical, automotive and civil). These independent checks often include physical tests and 'rule-of-thumb' calculation checks to catch gross errors.

On validation of the programs, packages like NASTRAN have been in regular use for ~20 years. For routine use by a competent designer, they are fairly robust.

Simply adding a large safety factor is not a solution. for financial and performance reasons, the product should be as close to the bone as possible. A good analysis program and in-depth understanding of structural behaviour can give you a better product (or a product that will actually take off with its full load!).

Something you need to realize is that the safety factors generally fall into two catagories

1) Loads 2) structural failure

By better understanding the modes of failure etc, the SF on 2) can be reduced (and even more importantly, a surprise falure mode won't catch you out!). The SF on loads (1) is most often regulated and hence cannot be lowered. It is these SFs that 'protect' you. Mike

---

Re: Risks of CAD programs (RISKS-7.38)

Sam Crowley <astroatc!crowley@spool.cs.wisc.edu>
Tue, 23 Aug 88 16:56:50 CDT

> Alan Kaminsky, School of Computer Science, Rochester Institute of Technology
> Now for the RISK. With a detailed picture of the exact stresses and
> deflections on a particular structural member, the engineer can justify
> designing with a smaller safety margin...

The term "smaller safety margin" should be "known safety margin" and the term "large safety factors" should be "large estimated safety factors". When a guess was made at the amount with a generous safety margin tossed in, the exact safety margin is still unknown. An estimate of the safety margin could be made depending on the accuracy of the guess.

Sam Crowley astroatc!crowley

Can current CAD/simulation methods handle long-term fatigue analysis?

<attcan!utzoo!henry@uunet.UU.NET>
Wed, 31 Aug 88 23:08:24 EDT

> Metal fatigue can be calculated with a reasonable amount of accuracy.

It is possible that my information is out of date. However, Aloha Airlines might dispute the matter! If fatigue calculation for real structures under real conditions is indeed accurate and practical, it is not being used very widely, for some reason. I'd be interested to see references on this.

> Most aircraft design use a 10% to 20% safety factor. A safety factor of
> two would make an aircraft so heavy it would never leave the ground.

For structural weights, yes, 10-20% is normal. But what I was thinking of was fatigue life, which -- at least in the military aircraft that are the ones I know most about -- is treated *very* conservatively.

Henry Spencer U.Toronto Zoology uunet!attcan!utzoo!henryhenry@zoo.toronto.edu

---

Re: Vincennes and Non-Computer Verification

<attcan!utzoo!henry@uunet.UU.NET>
Fri, 26 Aug 88 23:04:02 EDT

> Indeed, **what happened** in the case of the Vincennes? Was the U.S.
> operating naval patrols in a war zone without air support? If so, why?

The underlying problem here is simply that today's US Navy is not built for environments like the Gulf War. Their air support is concentrated in a handful of big, expensive, conspicuous, vulnerable carriers that cannot be risked in the Gulf. If the Vincennes had had a Harrier parked on its helipad ready to go, that would have been different, but it didn't. In an area as small as the Gulf, things happen quickly and there is no time to call up distant support forces. It's not practical to maintain airborne patrols on speculation -- too costly, not just in money but in wear and tear on men and machines, and in outright accidental losses. (A significant fraction of the British Harrier losses in the Falklands

War were accidents not involving enemy action.)

Henry Spencer @ U of Toronto Zoology

Re: Computers and Gambling (RISKS-7.39)

Jim Frost <madd@bu-it.BU.EDU>
Sat, 27 Aug 88 13:58:50 EDT

It's my observation regarding modified electronic games:

| [games] "..appear to run legitimate amusement games but with the flick
| of a switch they are converted to gambling machines.
|
| Machines of greater sophistication are now starting to appear
| with a second switch that totally erases the computer program
| [sic] which runs the illegal games.
|
| If that happens we are powerless to prosecute."

Modified games must have some sort of mechanism (either mechanical or human) to pay off a win. The existence of such a mechanism, especially if it were mechanical, could be used as proof that the machine had been used for gambling. I'm not a lawyer so I can't speculate on how well this might hold up in court though.

jim frost

> [Assuming the machine is in the "gambling" state rather than the normal "non-gambling" state, authorized surreptitiously by some trusted agent, such a payoff "mechanism" could be a screen message that asks you to type in suitable identification and then show up at the cashier's office. If the program then immediately returns the machine to its normal non-gambling state, that could be rather hard to detect unless someone were looking for it explicitly. One can conjure up all sorts of variants on this topic, but the problem is a valid one. PGN]

Automatic Bank Procedures

"David A. Honig" <honig@BONNIE.ICS.UCI.EDU>
Thu, 01 Sep 88 13:09:15 -0700

My bank, Home Federal in Ca., has a policy of locking an account (at least to ATM transactions) after * 3 months * of inactivity. This policy is implemented automatically by their computers. You cannot even check your balance using your ATM card when this is in effect.

This happened to me a year ago, also: that time the ATM swallowed my card because my savings account was "inactive" for a year. I had been trying to access my *active* checking account. Several days later I got my card back, after going to the bank. I had to withdraw a dollar from savings, then redeposit, to reactivate it.

This time when I asked the bank person I spoke with if he could do this administrative No-Op over the phone. He asked his supervisor, and said yes. I had given only the following information: my name, checking and savings account-numbers, and the ATM-card-number. Furthermore, he had called me back at a number that was not my home phone.

The phone mediated account re-activation contrasts with their conservative, automatic security policy; on the other hand, it seems they have struck an interesting balance between security and customer convenience. That tradeoff is important to many computer RISKS.

David Honig, Dept of Info & Comp. Sci, Univ. of Ca., Irvine 92717

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 43

Friday 2 September 1988

Contents

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

Statistical reliability estimation criticized (Jon Jacky, RISKS 7.40)

Brian Randell <Brian_Randell%newcastle.ac.uk@NSS.Cs.Ucl.AC.UK>
Fri, 2 Sep 88 11:07:59 WET DST

Re: Jon Jacky's message, stating that:
>John Cullyer of the British Royal Signals and Radar Establishment ...
>said, "Let's throw out the 10 ** -9" - and many of the audience
>responded with enthusiastic applause. Someone asked if he would accept a
>failure probability of only 10 ** -4 or 10 ** -5 for nuclear weapons safety.
>He responded, "In the weapons area there should be no room for probability.
>If something is unthinkable, don't let it happen. You either certify it or
>you don't - one or zero."

I'm appalled by this comment, if it is reported as accurately as I fear it is!
Just because something is "unthinkable" doesn't mean that *any* particular
technology, such as certification, will *guarantee* that it will not happen,
and that no measures need be taken, or even considered, to allow for the

possibility of failure. (This is the sort of thinking which has "justified" the reported lack of planning in the UK for dealing with Chernobyl-scale catastrophes at nuclear power stations.)

I find the following attitude much more professional. (The quote comes from the review by Tom de Marco of "Principles of Software Engineering Management", by Gilb and Finzi, in IEEE Computer for August 1988):

> "We must quantify everything that matters to eventual project success or failure. Everything - particularly those product characteristics that we treat as unquantifiable (flexibility, "user-friendliness," net benefit, etc.) - must be scaled and targeted. Some of the quantifications will be "fuzzy" in Gilb's terms, but even fuzzy numbers are far better than no numbers at all. The very act of coming up with the best-effort quantification of these factors guides us towards success and knowing how well we are doing along the way."

Otherwise, how will the Cullyers of this world for example (i) choose between rival certification techniques, (ii) know when certification is "complete", or (iii) decide how to divide a finite budget between certification and complementary approaches to reducing the likelihood of having to experience, and apologise for, an "unthinkable" occurrence. (In fact I fear I know the answer - by blind faith and misguided eloquence!)

All this is not to say that naive unjustifiable quantification, such as often accompanies the bandying around of figures like 10 ** -9, any more professional. However the fact that such naivete occurs is no reason to abandon attempts to find means of making, justifying and intelligently using, quantified reliability assessments, even w.r.t. design errors, especially with systems whose failures would be truly catastrophic.

Brian Randell

Calling party identification

Mark W. Eichin <eichin@ATHENA.MIT.EDU>
Thu, 1 Sep 88 22:22:08 EDT

>... It is my observation that most people believe that "tracing a call" is
>still a difficult, time consuming process that cannot be done routinely. This
>story shows that it is a service phone companies offer to commercial
>customers, although I have not seen any reports of it also being offered to
>residential customers ...

I believe the New Jersey telco offered digital display of incoming number to private subscribers a year ago; here at MIT, with the installation of a 5ESS system with full ISDN support available to offices, the digital set automatically displays the phone number the call came from (if it was within MIT; apparently there isn't software in place to track calls from other switches yet, the display merely indicates "Outside"). The documentation for the dormitory phones included mention of a ``privacy code'' which meant dialing 65 before any phone number; the pamphlet with the phone didn't actually explain what the privacy code *did* however.

Mark Eichin, SIPB Member & Project Athena ``Watchmaker''

Calling party identification Phone number tracing

<TMPLee@DOCKMASTER.ARPA>
Thu, 1 Sep 88 22:42 EDT

Our local cable company must use the same kind of connection to the phone company that the pizza place mentioned in RISKS-7.42 does. They have several pay-by-view channels and a set of incoming phone numbers. To order a pay-by-view event all you do is dial something like 938-77xx where the xx is the "ordering" code for the particular movie or live event (local sports, etc.) you want. A computer answers the call and is somehow told where the call was from; it looks that up in a data base, finds the i.d. of your cable box and enables the show. (It goes on your bill, of course.) Rather clever, actually: no human operators and it works from either a dial phone or a touch tone phone. Don't use it much, and apart from misdialling the only "risk" I have is remembering to use line 1 rather than line 2.

Ted Lee

Calling party identification

<[anonymous]>
Thu, 1 Sep 88 19:57:52 xDT

While there is work going on to allow for the identification of calling parties by the callee, such systems are not generally implemented and won't be for some time to come. There are some limited test projects, but I don't believe that any large-scale operation of the sort implied is currently operational.

Most likely what is actually happening is that the first question people are asked when they call the pizza folks is "what is your phone number?" Then the computer operator punches that in and up pops all the info from any previous call. It is unlikely that they are receiving the calling party's number in realtime. It IS true that with some long-distance carriers' 800 callers numbers are made available to the callee, but this is done on a billing cycle basis (i.e., in the billing statement) and not in realtime. If it turns out the pizza folks ARE receiving the number ID in realtime, then they are in one of the test groups and one can't help but wonder how many folks in the area realize the ramifications of this all (see below).

Now, in the middle future the issue of the callee being able to receive the number of the caller will be a significant one for us all. The technology is being put into place. At first glance, many people might say, "Gee, how neat, I'll know the numbers of the phone solicitors who bother me." But think again. It would work both ways. Do you really want YOUR phone number recorded (and possibly later called back with solicitations, matched with addresses for mailings, etc.) whenever you call a business, possibly from your private line you only intend to use for outgoing calls, or from some friend's house or business from where you happened to make the call? If you make a business call from home, do you necessarily want the person receiving the call to immediately

have your home number? Do they have any right to that number rather than calling you back on the office number you might give them? There are a variety of complex ramifications.

Even worse, if YOU could see the callers' numbers on calls YOU receive, you might be disappointed at much of what you'd see. Most big solicitation businesses use special outward-calls-only trunking groups; you would frequently see undialable numbers like 012-4161 on your display. Such info isn't going to do you a lot of good without a lot of hassling with telco for info (which they might well be unwilling to give you).

And what about obscene phone calls and such? Won't this system help stop them? Well, maybe some dummies would get caught, but there are one hell of a lot of payphones out there and people could easily move from one to another indefinitely...

The issue of privacy of callers' numbers is thus more complicated than it might appear at first. Some proposals call for unlisted numbers not to routinely display on callee displays. Some other plans propose a control prefix (e.g. "*21") which you could dial before dialing a phone number if you want to block number display for that particular call.

All in all the issues involved are quite complex. The time to start thinking about them is now.

Automotive EMI - a personal experience

Scott C. Crumpton <NESCC%NERVM.BITNET@CUNYVM.CUNY.EDU>
Fri, 26 Aug 1988 09:51:42 LCL

There is a section of road that I frequently drive which comes within about 600 feet of a TV (ch 20) transmitter tower. Within a distance of approximately 1/4 mi of the tower, the cruise control on my 87 Volvo 240DL will not set properly. The "set" button acts like "resume", causing a normal rate of acceleration up to the previously set speed. This behavior is repeatable in this location, however I have not noticed any other symptoms or occurrences in other locations.

Considering the "success" that I have had getting minor problems (like cold start stalling) fixed at the local Volvo dealer, I don't think I'll be taking this one to them. I will probably attempt to fix it myself with some ferrite chokes and a little shielding.

---Scott.

The mental tyranny of a cash register

<denbeste@OAKLAND.BBN.COM>
Mon, 29 Aug 88 12:01:58 -0400

Last Saturday I was in a local mall, and being thirsty I went to a cookie-over-the-counter store which was handy, and ordered a "medium rootbeer", price listed as $.75. I proffered a dollar, and was given $0.19 change.

[It should be explained at this point that Massachussetts has a 5% sales tax. However, this would have fallen under the restaurant and meal tax, which also happens to be 5%.]

"Wait a minute", I said, "The sales tax on this should be 4 cents, not 6."

"I know. The cash register is broken. But that is what it says to give you, so that's what I have to do." [I suspect my memory may be making his words a bit different - please bear with me.]

"Give me the rest of my change!"

"There's no way for me to do that." I walked away snarling.

Actually, of course, he could just have hit "No Sale" and gotten two more pennies out of the till. But, having done so, at the end of the shift the till would have contained less money than the cash register said it should, and he would've had to make up the difference out of his own pocket. Given a choice between it being his money and being mine, he wanted it to be mine.

Both of us were trapped by a cash register which had been programmed for an 8% sales tax.

Now that I've cooled down, I'm not even sure that he thought it through to the point I gave two paragraphs ago. I think his reaction was merely: Do what the machine says, even if you KNOW it is wrong.

Editorial point: Shades of the Vincennes.
We are the elite - we understand, at least in principle, what goes on inside of virtually anything which is computerized. This makes us free - we know enough to know that the computer can be just as wrong as a person can, since a person decided ahead of time what it would do. It is only a machine, and is just as fallible as its creators.
But for those out there who truly have no idea what a computer is, it has become a kind of oracle or demigod: You follow its orders and you DO NOT QUESTION, because it is smarter than you. Perhaps this is why some people flatly refuse to use automated tellers at banks, and literally refuse to touch a computer keyboard even when urged. Those who mess with the gods get turned to spiders.
When put in a job-related situation where interaction with a computer is unavoidable, the computer truly becomes almost a deity: YOU DO NOT QUESTION. ("We are sorry, Mr. Thompson, but our computer says that you are dead. We do not do business with corpses.")

[Maybe I HAVEN'T cooled down, after all.]

Intoximeter risks

Andrew Vaught <29284843%WSUVM1.BITNET@CUNYVM.CUNY.EDU>
Thu, 01 Sep 88 13:33:56 PLT

{Taken from the 24 August 1988 Spokesman-Review without permission}

GASSED OR DRUNK? PRISONER FILLS 'ER UP

While official witnesses looked on, a Bonner County Jail prisoner swigged a paper cup full of gasoline last week in an effort to prove himself innocent of drunk driving. Sagle resident Barry Joe Raynor, 20, claims he was siphoning gasoline just before he was arrested for drunken driving last Jan 14, said his attorney Jonathon Cottrell. When the case goes to trial in 1st District Magistrate Court next week, Cottrell and Raynor will argue it was gasoline on his breath that lit up the scoreboard on Bonner County's intoximeter the night he was arrested.

[The article goes on to say why drinking gasoline is not a real good idea and how drinking a cup of gasoline showed a .28 percent blood alcohol level one hour later.]

Although the article never mentions what kind of `intoximeter' is actually used in the tests, it is pretty obvious that it is not directly measuring blood alcohol content, but some other telltale that allows it to be fooled by gasoline.

[NPR this morning noted that when the tape recording of the arrest was played in court, Raynor sounded so intoxicated that he simply gave up on his gas defense. OK. This item thus appears to not be RISKS related, although the risk of false positives on such tests is always a risk that must be recognized. PGN]

SSNs, Passports

<Hibbert.pa@Xerox.COM>
Wed, 31 Aug 88 17:45:40 PDT

I was just looking through Robert Ellis Smith's "Report on the Collection and Use of Social Security Numbers", and on the final page he added a note about SSN's and the Passport office. Since there was some unresolved discussion of this at the beginning of the year, I thought I would forward the information.

Smith says that as of the beginning of this year, SSN's are required on passport applications, and failure to include it may result in a $500 fine. I'm as puzzled by this as the people who reported similar things in January. I don't know why the passport office doesn't refuse to handle applications without SSNs and just forget about the fine.

The reason they want the number in the first place is apparently so that the IRS can make sure that Americans living abroad file returns.

If there really is a fine, then it should be mentioned in the requisite Privacy Act notice along with a statement as to whether disclosure has an impact on you're getting a passport.

The "Report on the Collection and Use of Social Security Numbers" can be

ordered from the Privacy Journal, P.O. Box 15300, Washington DC 20003. Their phone number is (202) 547-2865. I was dissapointed in the level of the report. It's mostly a sampler of case histories of people who were burned in various ways by abuse of their numbers. It contains little in the way of privacy advice that hasn't already appeared here.

Chris

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 44

Monday 5 September 1988

Contents

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

Re: "Pizzamation"

Bob N. Mayo @ U.W. Madison Computer Sciences <mayo@cs.wisc.edu>
Sat, 3 Sep 88 13:17:29 CDT

Godfather's Pizza [phone (206) 223-1111] claims that they don't get told the customer's phone number. This contradicts the previous article which claims that they automatically receive your number, that is then used to display your "pizza-history".

When I called them to ask about this, Godfather's claimed that they ask you for your phone number and then set up an "account" for you. They specifically stated that they do not automatically receive customer's phone numbers.

Can anybody account for this discrepancy? I can think of several possibilities:

+ The previous article was in error.
+ They have discontinued this practice. (Perhaps due to poor reception from the public?)
+ Godfather's didn't tell me the truth.

Anybody know?
--Bob

[Most likely the first one. PGN]

Re: Pizzamation and FGD lines...

Edwin Wiles <netxcom!ewiles@uunet.UU.NET>
Sat, 3 Sep 88 02:08:10 EDT

On a standard telephone line, it is still difficult to 'trace a call'. In all probability these businesses are using what are known as "Feature Group D" lines; which have aprox 6 to 8 wires, as compared to the 2 to 4 wires of a normal telephone line.

Feature Group D service is designed to tell you both the number dialed, and the number that is doing the dialing. The extra lines are used for signaling the address information.

[I know whereof I speak, our company is using FGD lines, and I had to design a program to interface with the phone company protocols. Not easy....]

Yes, personally I would like one of these lines, with a smart phone to block unwanted calls. However, such phones already exist, that work over standard phone lines, the caller simply has to punch a few more digits (like a PIN) to let your phone know that they are allowed to talk to you. The nice thing about a FGD line, is that you can reject the call without actually having answered it, thereby allowing the caller to avoid paying the phone company for a call that you'd reject anyway.

Edwin Wiles, NetExpress Comm., Inc., 1953 Gallows Rd. Suite 300 Vienna, VA 22180

Automatic Number ID: Great Idea!

<sun!portal!cup.portal.com!Patrick_A_Townson@unix.SRI.COM>
Sat Sep 3 13:25:31 1988

[Note: This address for PAT is bogus, and does not work. Try "sun!portal!cup.portal.com!username"@Sun.COM or "sun!portal!cup.portal.com!username"@uunet.UU.NET]

A recent article here by Anonymous warned of the 'dire consequences' all of us would face when Automatic Number Identification on a real time basis became a routine feature.

I have to disagree, wholeheartedly. ANI will be one of the best, and most useful additions to telephony that I can think of.

I consider an unsolicited phone call to be an invasion of my privacy. If you feel you have the right to call me and refuse to identify yourself, then I maintain I have the right to come to your front door and refuse to identify myself.

While it is true, as Anonymous pointed out that phone solicitors and the like frequently work from phones with special types of circuit numbers which cannot be easily traced by someone with ANI, the fact remains that ANI will bring a virtual halt to most of the hacking and phreaking and obscene calls which plague many people. Yes, as Anonymous points out (an appropriate handle, considering the gist of his message, no?) people can move around from one payphone to another, endlessly, continuing to create their havoc in whatever form it takes, but in reality, most people will not take portable modems and terminals with them to the pay phone on the corner just so they can call someone's BBS and harass them Anonymously.

Having ANI implemented will simply make it too inconvenient for most of the low-life scum who hide behind their telephone to continue their practices. As for legitimate reasons to not want your number displayed to the called party, I can't think of any. Again, you have to make the analogy of going to see someone in person. It is completely unfair and unrealistic to say that you have the right to disturb someone at whatever they were doing and that they in turn have no right to demand to know who you are.

In summary, I believe you have the right to use the phone as a method of quick, almost instant communication with others. You do not have the right to use the phone as a way to remain Anonymous. Having a non-published number is a different matter altogether, since you are protecting yourself against persons who might call you. The way you protect your privacy when calling someone else is to *simply not make the call at all* if there is something which will be said which you would not want traced back to yourself.

Anonymous is also making the assumption that the people who aquire your number via ANI will automatically abuse the information. This is mostly false.

If and when ANI at the subscriber level becomes available here in Chicago, I will be one of the first to subscribe. And when a call is received and the read out shows that the person has deliberatly blocked their number from my view, I will probably answer the phone and state that they are welcome to call back making the information available, and pending that action, the present call is being terminated now. (click).

Patrick Townson

COMPASS REPORT in RISKS 7.40

Brian Randell <Brian_Randell@newcastle.ac.uk>
Mon, 5 Sep 88 16:11:01 WET DST

Here are comments by Prof. Bev Littlewood - unfortunately not a RISKS reader - on Jon Jacky's report from COMPASS 88, which I am posting to RISKS on his behalf.

To Brian Randell:

>The recent report of COMPASS 88, if accurate, contained some pretty shocking
>things. John Cullyer is quoted as saying "Let's throw out the 10**-9", a view

>that brought audience applause. He went on to say, when questioned about
>nuclear weapons safety, that "in the weapons area there should be no room
>for probability. If something is unthinkable, don't let it happen. You
>either certify it or you don't - one or zero."
>
>The last sentence worries me. He appears to be asserting that it is possible
>to certify (note that word) that a system is perfect (i.e. that the unthink-
>able will not happen). Does he really mean this? What about design flaws,
>specification errors? It seems to me that this attitude, prevalent on the
>wilder fringes of the formalist community in the UK, seeks to turn a wish
>into a fact. Of course, we would all like to be able to remove the uncertainty
>which is present in the process of building systems, but that uncertainty
>is a fact of life. There is an intrinsic limit to the extent to which we
>can formalise the problem domain, even if we are successful in current attempts
>to formalise later stages of design.
>
>If an element of uncertainty is inevitable, we need a calculus of uncertainty.
>The only one we have is probability (see, for example, de Finetti on the
>'inevitability' of probability as a means of describing uncertainty).
>
>Nancy Leveson's remarks are just as bad, although possibly more amusing.
>Nancy told the story of her encounter with an engineer who wanted to know
>what number to fill in for the probability of the event labelled "software
>failure" on a fault tree. Leveson tried to explain that there was no number
>but he persisted. Finally she answered, "Just write 1.0."
>
>Leveson is LITERALLY correct - the software will ultimately fail with certainty
>- but the engineer is asking a responsible question. He wants to know how
>frequently the software will fail so that he can make scientifically informed
>judgements to aid in the engineering decisions he must take.
>
>There is a lot of confusion in this area, and some of it seems to centre
>around figures like 10**-9. Many people do not seem able to distinguish
>between such a figure being MEANINGFUL (which it is), and being ACHIEVABLE
>(which it probably isn't) and ASSURABLE (which it certainly isn't).
>
>Consider the 10**-9 failures per hour for the Airbus A320 fly-by-wire system.
>This is often taken to be 'meaningless' because it is so small. However, if
>we assume aircraft fly 5000 hours each year, that each has a 20 year life, and
>that the fleet size is 1000, we arrive at a 100,000,000 hours in the air for
>the fleet life. 10**-9 then translates into an approximate 1 in 10 chance
>of failure in the life of the fleet. This is an 'ordinary' probability
>which is meaningful to anyone and could, for example, be used as part of
>a calculation to fix insurance rates (I wonder how they were actually fixed?).
>
>Digressing for a moment, it is interesting in the case of the A320 that the
>manufacturers are on record as stating 10**-9 per hour is a REQUIREMENT for
>this system (because, again as they say, failures cannot be tolerated). It
>is obvious that achievement of this 'requirement' has not been demonstrated,
>and one wonders how reliable the system actually is. Presumably it falls
>far short of 10**-9. This presents a difficulty, because the manufacturers
>were so confident of their ability to make it sufficiently reliable that they
>did not provide a fully functioning mechanical back-up for use in the event
>of complete system loss. If this were to occur, the pilot only has trim and

>rudder to fly the aircraft. The aircraft has been landed in this configur-
>ation, but I am told that it is not easy (an understatement) and airline
>pilots will not be trained for such landings.
>
>Returning to the main theme, I think that probability statements representing
>very high reliabilities are meaningful and necessary for safety-critical
>systems. But, of course, I agree with Miller that they are essentially
>inpossible to measure and so in practice we shall not be able to assure
>ourselves that we have achieved what is necessary (even if, by some miracle,
>such a reliability had in fact been achieved).
>
>Thus far I suppose we are not in too great disagreement with the likes of
>Cullyer and Leveson. It is when we start to consider the implications of
>our inability to assure very high reliabilities that we start to differ.
>They seem to think that this is due in some way to defects in statistical
>methodology and that we should therefore have no more truck with statistics
>(and statisticians?). In fact, of course, the problem is due to the intrinsic
>paucity of information about such systems, when compared with the very strong
>statements we wish to make. Improvement of statistical methodology will not
>be able to dent this problem. But that does not mean that Cullyer-type
>'certification' can be used instead (unless he means by this a assurance that
>the failure rate is ZERO - and I do not believe this is the case). Rather
>it means that we are in a genuine impasse, and perhaps ought to face the
>unpalatable view that we should not be building systems which require a
>reliability which is not assurable.
>
>
>Bev Littlewood, Centre for Software Reliability, The City University, London.
>
>email: sd396@city.ac.uk
>
>

--
Brian Randell, Computing Laboratory, University of Newcastle upon Tyne

JANET = Brian_Randell@uk.ac.newcastle
ARPA = Brian_Randell@newcastle.ac.uk
UUCP = ...!ukc!newcastle.ac.uk!Brian_Randell
PHONE = +44 91 222 7923

Statistical reliability estimation (Brian Randell, RISKS 7.43)

Lance J. Hoffman <LANCE%GWUVM.BITNET@CUNYVM.CUNY.EDU>
Fri, 2 Sep 1988 20:00 EDT

> "...The very act of coming up with the best-effort quantification of these
>factors [flexibility, user-friendliness, net benefit, etc.] guides us
>towards success and knowing how well we are doing along the way" - Gilb and
>Finzi, quoted by Randell

This is certainly true. In the majority of risk analyses I've seen, the end product was secondary to the learning process that took place as people did it (and often implemented immediate simple fixes along the way). There is, however, a quasi-religious debate between the quantitative types and the qualitative types. Moreover, the issues of risk perception and risk communication often dominate the technical issues (and, in my opinion, properly so). Stu Katzke of NBS and Sylvan Pinsky of the National Computer Security Center have developed an initial risk model for computer security, which is published in Proc. 1st Risk Model Builders Symp., Martin-Marietta, Denver, 1988. Copies of the entire proceedings will be given out, I am told, to attendees at the upcoming Baltimore computer security conference sponsored by NBS and NCSC. And much food for thought if found in a journal I find that few computer security types get, Risk Analysis, published by the Society for Risk Analysis, published by Plenum Press. It is the official journal of the society, 8000 Westpark Drive, Suite 400, McLean VA 22102 (says the masthead). Many of the authors of papers here have been working on computer and noncomputer risks for a long time.

Sample articles from the 9/87 issue: Impact of AI on the Risk Analysis Profession; Informing and Educating the Public about Risk; Book Reviews; Software Review (WHAZAN, for assessing chemical process hazards); and more. You get the idea.

- Lance Hoffman, George Washington University (LANCE@GWUVM.BITNET)

Re: Calculations with wrapped numbers

Bruce Karsh <karsh@sgi.com>
Fri, 2 Sep 88 20:51:28 PDT

> The problem occurs when the previous value is -175 or so and the new
> value is +175. What is the average? Adding and dividing by two doesn't
> cut it (zero is certainly NOT the answer).

> I don't remember how we solved this particular problem, but I have thought
> about it since then. Imagine trying to compute the average position of the
> second hand on a clock. You sample the position once a second for sixty
> seconds. Ok, now what is the average?

A good way to estimate an average angle, A, from a set of angle measurements a[i] 0<=i<N, is:

$$a = \arctan\left(\frac{\sum_{i=1}^{N} \sin(a[i])}{\sum_{i=1}^{N} \cos(a[i])}\right)$$

A very careful study of the properties of this estimator is in the book "Statistics On Spheres", Geoffrey S. Watson, University of Arkansas Lecture Notes in the Mathematical Sciences, 1983 John Wiley & Sons, Inc.

The importance of this to RISKS is that the problem of computing an average angle comes up all the time in computing. An answer to the problem was published at least as long ago as 1983 and probably known for a long time before that.

Yet people try to calculate average angles in all kinds of ways, too many of which give terribly wrong answers!

The problem is that the people who design and program software are not always aware of the techniques that they need to make correct programs. There are untold thousands of computational techniques, ... certainly more than we can expect people who program numerical methods to know.

The average angle problem is not the only one that people regularly program incorrectly. A recent discussion in comp.graphics illustrated how frequently wrong solutions are given to the problem of calculating whether or not a point is inside a polygon. Similarly, people regularly code incorrect procedures which purport to determine whether or not two line segments intersect.

We need to better reference materials on numerical methods. Most numerical methods books concentrate on finding solutions to {differential, linear, integral, ...etc} equations and on computing values of special functions. But we need references on less classical problems. For example, how many more times are people going to program bad solutions to the point-in-polygon problem? How many system failures are we going to tolerate because of wrong solutions to the line intersection problem? We need to be able to look up solutions to these problems.

Of course, if such a reference book were produced, how many programmers would actually use it?

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 45

Wednesday 7 September 1988

Contents

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

"Cheater software"

Rodney Hoffman <Hoffman.es@Xerox.COM>
6 Sep 88 08:06:50 PDT (Tuesday)

>From a story by Kim Murphy in the Sept. 3 'Los Angeles Times':

> General Dynamics Corp. was accused of using "cheater software" and other fraudulent practices to falsify tests and supply defective components for the U.S. Navy's Phalanx anti-missile gun system and the Standard Missile program.
>
> In a lawsuit filed in Los Angeles federal court, one former and four current General Dynamics employees -- technicians, supervisors and quality-control specialists -- accused the St. Louis-based defense contractor of encouraging its employees to engage in widespread test

falsifications that may have compromised the integrity of the two weapons systems....

A "cheater software" computer program allows company technicians to begin running a test, then abort it and obtain a passing reading, the suit contends....

[more on other, non-software-related means used to falsify tests]

"COMPASS REPORT in RISKS 7.40 (Bev Littlewood via Brian Randell)"

<leveson@electron.LCS.MIT.EDU>
Tue, 06 Sep 88 16:58:42 -0400

Wait a minute. I have been tarred with an opinion that I do not have and have never espoused.

>Nancy Leveson's remarks are just as bad, although possibly more amusing.
>Nancy told the story of her encounter with an engineer who wanted to know
>what number to fill in for the probability of the event labeled "software
>failure" on a fault tree. Leveson tried to explain that there was no number
>but he persisted. Finally she answered, "Just write 1.0."
>
>Leveson is LITERALLY correct - the software will ultimately fail with certainty
>- but the engineer is asking a responsible question. He wants to know how
>frequently the software will fail so that he can make scientifically informed
>judgments to aid in the engineering decisions he must take.

I did not say his question was irresponsible, only that it was unanswerable at this time with the confidence that he wants. Since we cannot measure such low reliability numbers, then these types of systems should not be built to depend on the correct operation of the computer, i.e., the fault tree should take the conservative view of assigning 1.0 to the probability of failure of the software and, therefore, the builders will be required to show that the system is safe even if the software fails. For example, a fully automated nuclear power plant safety system or fly-by-wire aircraft might be considered safe enough if there are usable and reliable back-up systems that do not rely on proper operation of a computer. The problem with the Airbus 320 appears to be that they are relying on the computers and not taking the need for back-up systems seriously. The same, unfortunately, is also true for the nuclear power plant design that the engineer I was speaking with was evaluating.

>Thus far I suppose we are not in too great disagreement with the likes of
>Cullyer and Leveson.

How did my opinions on the subject (which were never stated in the original message from Jon Jacky) and John Cullyer's get lumped together? I am not usually accused of agreeing with anyone :-).

>They seem to think that this is due in some way to defects in statistical
>methodology and that we should therefore have no more truck with statistics

>(and statisticians?).

I have never made such a statement or implied this. I am in favor of research in software reliability (and safety) measurement and in its use currently for systems that do not involve loss of life and therefore do not require very low numbers and high confidence.

>Improvement of statistical methodology will not
>be able to dent this problem. But that does not mean that Cullyer-type
>'certification' can be used instead (unless he means by this a assurance that
>the failure rate is ZERO - and I do not believe this is the case). Rather
>it means that we are in a genuine impasse, and perhaps ought to face the
>unpalatable view that we should not be building systems which require a
>reliability which is not assurable.

Most systems are not 100% safe, nor does society require them to be. We usually require only an acceptable level of safety. The problem is in Bev's equating failure-free and safe. Making them failure-free would certainly work, but it is not necessary. For example, aircraft are not failure-free, but they seem to have a safety level that is acceptable to society. What we need to eliminate is catastrophic failure modes, not necessarily ALL failure modes. If we had to do the latter, we would need to abandon much of current technology. I personally feel that there are other solutions (which I have written extensively about) than just not building systems with computers. That is, I believe we can build adequately safe systems without requiring 10**-9 reliability. Unfortunately, not many software engineers know enough about system safety to build such software systems and the system safety engineers do not understand computers.

JANET = Brian_Randell@uk.ac.newcastle

Automatic Number ID: Great Idea! (RISKS-7.44)

Jerome H. Saltzer <Saltzer@ATHENA.MIT.EDU>
Tue, 6 Sep 88 13:47:33 EDT

In "Automatic Number ID: Great Idea!", Patrick Townson makes several good arguments favoring Automatic Number Identification (ANI). I agree that on balance ANI will be a good thing once the novelty wears off and people become accustomed to the new rules of the game. But Townson may be carrying a good argument a little too far when he says,

> As for legitimate reasons to not want your number displayed to
> the called party, I can't think of any.

I assume that he took that somewhat polar position in order to draw out suggestions for legitimate reasons, so here are a couple of cases in which maintaining the privacy of the caller does seem to make some sense:

1. Hotlines (e.g., drug-abuse and suicide) and police

department tip numbers depend on anonymity of the caller to perform a function that is usually considered to have some value to society. Some police departments maintain a line separate from 911 (which often has an ANI feature) just for this purpose. If the caller of a hotline knew that the calling number would be automatically recorded, at least some of the information that flows in this way would dry up, and some of the help dispensed this way would not be. (The technique of dialing a prefix code to block automatic number identification caters to this requirement. I doubt that many hotlines would take Townson's hard-nosed approach and refuse to accept a call from a prospective suicide who has blocked ANI.)

2. When a private party calls on a "big organization," (for example, making ten queries to stock trading companies about their commission rates in anticipation of opening one account) there is an understandable preference for not leaving one's number, simply to avoid unwanted followup calls (e.g., from hungry brokers). Again, the ANI-blocking prefix satisfies this requirement, because no hungry stockbroker is going to refuse a call that sounds like it comes from a promising prospect.

Townson's polar position might be plausible if you assume telephones are answered only by private individuals. He is well-advised to refuse anonymous calls to his bulletin board and welcome to refuse them at his private phone. But I believe that the need for blocking ANI remains for other situations.

Jerry

Re: Display of telephone numbers on receiving party's phone

Bruce O'Neel <XRBEO%VPFVM.BITNET@CUNYVM.CUNY.EDU>
Tue, 06 Sep 88 17:30:25 EDT

I much prefer using a prefix (*21 say) only when you WANT the number to be known, rather than when you DO NOT want the callee to see it.

bruce

Re: Telephones and Privacy

C H Longmore <CCAse7-16@birmingham.ac.uk>
Tue, 6 Sep 88 20:28+0100

Patrick Townson's article in RISKS 7.44 states:

> Having ANI implemented will simply make it too inconvenient for most of the
> low-life scum who hide behind their telephone to continue their practices.
> As for legitimate reasons to not want your number displayed to the called
> party, I can't think of any. Again, you have to make the analogy of going

> to see someone in person. It is completely unfair and unrealistic to say
> that you have the right to disturb someone at whatever they were doing and
> that they in turn have no right to demand to know who you are.

How could you apply this to a situation where [as in the UK] certain police forces operate systems whereby people can give information to the police *anonymously* by calling a device as simple as an answering machine?

How could you apply it to a situation where a potential customer wishes to obtain a quote by phone *without* running the risk of that company using the information so gained to apply the hard-sell.

Can you imagine someone using a confidential medical advice line (such as an AIDS advisory service) if there was a possibility of the call being easily traced?

How many people would telephone up the Samaritans if their number wasn't confidential?

In the UK these are not problems.... yet. Our current telephone network is not capable of supporting these features.... yet.

It *should* be possible to conceal your own telephone number from the person you are calling.. however, it is also the right of the person receiving the call to refuse to communicate with anybody who does not want his/her telephone number revealed. The latter is easy enough to implement.... a simple user-settable switch on the telephone is all that is needed.

The 'privacy' argument has two sides.... it is the right of an individual *not* to have their phone number displayed, but it is also the right of the individual *not* to answer anonymous calls. A problem to which the solution seems easy enough.... (now prove otherwise!)

Conrad H Longmore
Computer Science Dept, University of Birmingham, Birmingham B15 2TT, UK.

email: CCAse7-16%multics.bham.ac.uk@cunyvm.cuny.edu

Gambling with video arcade machines

<Mike.Blackwell@ROVER.RI.CMU.EDU>
Tue, 6 Sep 1988 17:34-EDT

I was once called to be an expert witness in a case involving gambling with video poker machines. The case never went to trial, but I did gain some insight as to how they work.

In a typical video card machine, you put in your quarter, and earn one card hand (five card draw or blackjack are the most common). You play the hand (discarding and drawing new cards - no betting here, you just get one shot), and at the end win so may points for your final hand (from zero for a bad hand, one for two-pair, two for three-of-a-kind,

up to maybe 500 for a royal-flush). In a real gambling machine (like in Vegas), you'll get quarters for your points - they spit right out of the machine. In a non-gambling arcade machine, you just get free games for your points. This is legal, no different than winning free games or extra time at Space Invaders (in Pennsylvania, at least, playing video poker is considered to require skill...).

What makes the arcade style card machine a gambling device is the addition of a "knock-off" switch. This is a switch, either directly on the machine, or wired from the bar, which zeros out the any free games. How it works is you rack up your zillion free games, find the barkeeper (or whoever, but this seems to usually take place in bars), and he'll pay you one quarter for each free game you've won. Then he'll clear the free games from the machine. It is solely the presence of this knock-off switch that classifies the machine as a gambling device. Apparently (though I was never able to confirm this), simply power cycling the machine does not clear free games.

Even if a bar is not caught paying off, the game distributor can be tried for providing machines with knock-off switches.

-m-

Video Games

Ed Nilges <EGNILGES@PUCC.Princeton.EDU>
Tue, 06 Sep 88 13:27:04 EDT

How many computer professionals have noticed the continual technical improvement of video games in the past couple of years, and the concomitant decline of their social and moral content? Nintendo and other Japanese companies, with little knowledge or care about the effect of racial tensions on American cities, market games such as Ninja Warriors vs. Bad Dudes, which feature a Caucasian-looking (or Japanese) hero, fighting black villains. The video game user manipulates the characters in a seedy back-alley environment featuring garbage cans and rats...an offensive comment, on the face of it, on the state of the inner city.

Other games allow players to act as contra rebels or air force pilots, without teaching them either the misery of dying in a jungle, or the difficulty of qualifying to be an Air Force enlisted man, let alone pilot.

The graphics are beautiful: the content is vile. Surely it's our responsibility as computer professionals to protest this application of a technology which could improve lives. While the Japanese are to be applauded for making technology affordable, they are to be condemned for taking technology developed in the US, and using it to degrade people in this way.

Perhaps the most effective thing for computer people to do is to

approach restaurant owners in their own community who operate such machines and explain their concerns as professionals and, if applicable, as parents. Video game parlor operators are obviously not going to listen, but restaurant owners may.

Re: Wembley-on-the-Motown (RISKS 7.42)

Jeffrey R Kell <JEFF@UTCVM.BITNET>
Tue, 06 Sep 88 10:11:27 EDT

(I play keyboards/synthesizer part-time aside from my "real" job...)
Any electronic musical equipment, especially anything constantly moved with a traveling show, is far from being highly reliable. The newest electronic keyboards are probably the most sensitive of all. You are fortunate to get predictable results in a controlled (studio) environment, let alone have a delicate piece of equipment be thrown around by the road crew, plugged into unstable power sources and subjected to varying temperature conditions.

Original synthesizers (Moog, Arp) with their knobs, switches, and patch cords took some time to set properly, but they did STAY SET, other than perhaps small tuning adjustments. The second generation could record these settings in small internal memories, thus making the first synthesizer "programs". The third generation was practically all digital (notably Korg, Yamaha) with settings programmed as parameters, and internal memory grew to several K-bytes of RAM, often with battery backup and cassette backup. The latest generation recreates sounds from digital samples, much like a CD Disk player. The Synclavier mentioned is one of the top-of-the-line of these types. I own a Korg DSS-1 (standard disclaimers) which has 768K RAM, a 3.5 diskette drive, and can turn out a 48KHz sample rate at 14 bit resolution. Very nice, but one minor power glitch and memory is lost must be rebooted (about 30 seconds, but rather annoying in the middle of a song). I was once stuck on an out-of-town job with two third-generation Poly-800's which were packed by a member of the road crew and inadvertently left turned on (they can operate from batteries alone) resulting in loss of memory (and cassette backup at home).

The risk of high-tech music can also be heard in CD disks. They sound superb when they work, but go far off into the ozone when they fail. Quite a far cry from the brief bump of a phonograph needle skipping a groove.

I have caught myself longing for the days of the trusty piano which, with a tuning or two a year, always got the job done. At least in that respect, I find it easier to relate to the techno-phobes who distrust automation.

Jeffrey R Kell, Dir Tech Services, Admin Computing, 117 Hunter Hall,
Univ of Tennessee at Chattanooga, Chattanooga, TN 37403

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 46

Wednesday 7 September 1988

Contents

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

Airbus vs U.K. MOD development standards

<PROCIS@ICNUCEVM.BITNET>
Wed, 7 Sep 88 18:31 SET

From "Systems International", August 1988 issue, editorial page: "In his recent lecture entitled "Should we trust computers?" given to the British Computer Society, Martin Thomas, chairman of Praxis, said ..... the computer systems used on the ill-fated A320 at the Paris Air Show were developed using techniques 'the UK Ministry of Defence would find unacceptable for safety critical _military_ software in the future'". Can anyone give a first-hand account of that lecture, or a more complete citation, or somehow shed more light on the issue? I am curious about a) how far that future is; b) which of the new rules would the A-320 development violate; c) how many current systems would be found to violate those rules, and how many to respect them.

Lorenzo Strigini

Vincennes: Rules of engagement violated by AI heuristic?

Clifford Johnson <GA.CJJ@Forsythe.Stanford.EDU>
Wed, 7 Sep 88 00:00:32 PDT

A recent contribution noted that the Airbus shot down by the Vincennes had been within binocular range of the ship, and inferred that binoculars were superior to the Aegis system. This is invalid. Reportedly, there was an obscuring haze, and, besides, even had the plane been identified as an Iranian Airbus, it would have been shot down, according to the Pentagon's latest report, which states that the Captain was fully aware that the plane may well have been a commercial flight, e.g.: "On the Vincennes, an officer watches the plane slowly rising. He jumps to his feet and says 'possible comair,' for commercial aircraft, to the ship's commanding officer, Capt. Will. C. Rogers. The Captain acknowledges this." (See NYT, Aug.20, for this and the other info. I report.)

Another contribution citing the Vincennes noted the tendency for computer output to be definitive, right or wrong. This analogy is valid. It was not the Aegis giving bad data, but it was the Aegis giving a procedurally *conclusive* categorization, together with the duty-imposed rules of engagement, that caused what the military now boasts was a "prudent," albeit automatic, killing of 290 civilians. Thus: (1) from the moment of take-off, the plane was formally characterized as hostile merely because the airfield was not wholly civilian, and this characterization would be definitively "correct" until disproven by the flight's obeying the ship's radioed warnings; (2) the rules of engagement next required that protection of armed-to-the-teeth U.S. militia have top priority, above protection of defenseless civilians in transit. (Since the latter protection was the purported mission of the Vincennes, this seems to me a code of cowardice rather than a rule of engagement.) These rules required the shootdown. The Aegis did its job and the Captain his mandated duty, and they conclusively saved the Vincennes from the risk posed by a lumbering Iranian Airbus that would not immediately respond to radioed warnings.

JCS Chairman Crowe explained that all fault lay with Iran, because it was "unconscionable" for the Iranians to permit a civilian airliner to take off amid hostilities (which the air controllers are simply presumed to have known about) and to ignore warnings. According to the NYT, Crowe asserted that the plane would have been shot down IN ANY CASE given lack of proof that it was not hostile. Such "shoot-on-suspicion" rules of engagement Crowe claimed to be wise policy. (To me it is chilling that the U.S. calls the shootdown a commendable "We'd-do-it-again" preprogrammed procedure, rather than a wildly mistaken massacre; this kindles memory of Reagan's ire after the KAL007 shootdown: "Shooting down a plane, even one with hundreds of innocent men, women, children, and babies, is part of their normal procedure.")

The Pentagon's support of the shootdown as a prudent necessity fails to address the official notice provided by the U.S. re its rules of engagement in the Gulf, which stated: "United States Navy ship captains realize that not all commercial aircraft transmit their proper IFF code or remain in the proper airways and will take this into account when they encounter such an aircraft." So it seems a post-facto revision of the rules of engagement to assert that

failure to respond to warnings is per se sufficient cause for deadly force *until proven otherwise*. That is, Rule Of Engagement number (1) above was in violation of the declared Rules Of Engagement. The U.S. should have informed the airlines that all planes taking off from Bandar Abbas were presumed hostile until proven otherwise, instead of informing them that no such presumption would apply even if such a plane strayed from its corridoor and failed to broadcast civilian codes, let alone if it was within its corridoor and did emit civilian codes.

One natural question naturally not commented on in the Pentagon's report is the applicability of the word "panic," although it notes: "At every opportunity when the ship's internal communication link is silent, an officer known as the tactical information co-ordinator calls the attention of the other officers to his belief that the plane is accelerating and descending. His computer terminal, like others on the ship, actually shows the aircraft rising... 'Towards the end,' wrote Gen. George B. Crist, 'it is reported he was yelling out loud.'" By not even reprimanding this officer, and by ultimately blaming inadequate but correctable video displays, the Pentagon is materially announcing that misreading computer consoles is an accepted, large risk that higly-trained crewmen cannot be expected to avoid, and which absolves Captain, crew, and computer from all responsibility.

Interest has been expressed in the numerical/logical algorithms whereby computerized sensors declare a detection as hostile. The above illustrates that declaration of hostility is not merely a simple sensor in-/de-duction, but as much an "IF-THEN" heuristic/rule-of-thumb, e.g.: "IF TAKE-OFF FROM NOT NOT MILITARY AIRFIELD AND ALERT-LEVEL ABOVE 2, UNTIL AFFIRMATIVE RADIO RESPONSE THEN BLIP IS HOSTILE THEN SHOOT ON APPROACH." What is ordinarily construed as objective inference, is in fact a mandated conditional *definition*. (Likewise, it is linguistically predefined that the United States is "under attack" -- which triggers and authorizes retaliation -- if a nuclear attack warning level exceeds a certain threshold, euphemistically dubbed "the President's Launch Under Attack threshold".)

Re purely statistical sensor detection, I recommend "Data Fusion" in Defense Electronic's first annual C3I Handbook (1986). It provides a comprehensive table of techniques, which include Bayesian, frequentist, maximum likelihood, evidential, pattern-matching, associative, syntactic, and heuristic methodologies. A basic division is into "hard" sensors, that declare an attack in binary form (yes/no), and "soft" sensors, that provide a probability estimate that a detection is hostile.

Re: Statistical reliability estimation and "certification"

Jon Jacky <jon@june.cs.washington.edu>
Wed, 07 Sep 88 08:43:03 PDT

Postings by Brian Randell, Bev Littlewood and others responding to my COMPASS trip report suggest that some clarification may be required. I am confident that I quoted Cullyer, Leveson and others accurately; I took careful notes on the spot. However ---

- I should emphasize that skeptical comments regarding statistical reliability estimation were limited to the context of *a priori predictions* of the reliability of *software* - that is, predicitions of software reliability made prior to experience in the field. Regarding their opinions on statistical reliability estimation and life in general, I cannot say. I did note that Cullyer and others did remark that a priori estimates could be useful for *hardware* systems, where failure histories for the components were known.

- - There seems to be a misunderstanding regarding the term "certification" - in particular, Cullyer's remark that "you either certify (a product) or you don't - - one or zero." Apparently some readers understood "certification" in this context to refer to some formal validation technique, which Cullyer was claiming was "perfect" in some sense. I believe that was not the intended meaning. It is necessary to distinguish *validation* from *certification*. Validation is the technical process of determining whether a product conforms to its requirements. Nobody at COMPASS claimed that any validation technique was perfect, although people did claim that some techniques were better than others. Certification is the administrative act of releasing a potentially hazardous product for sale or use. Certification IS one or zero. The necessity for basing a yes-no decision on less-than-totally-conclusive technical information is the certifier's dilemma.

- Jonathan Jacky, University of Washington

A Computer Virus Case Goes to Trial

Joe Morris (jcmorris@mitre.arpa) <jcmorris@mitre.arpa>
Wed, 07 Sep 88 13:05:09 EDT

From the _Washington_Post_, 7 September 88, page C-1 (without permission):

JURY SELECTION IN 1ST `VIRUS' TRIAL BEGINS (AP)

Fort Worth, Sept. 6 -- Jury selection began today in the criminal trial of a 40-year-old programmer accused of using a computer "virus" to sabotage thousands of records at his former work place.
The trial is expected to last about two weeks.

Donald G. Burleson faces up to 10 years in jail and a $5,000 fine if convicted in the trial, a first for the computer industry. Burleson was indicted on charges of burglary and harmful access [sic] to a computer in connection with computer damage at a securities firm, said Nell Garrison, clerk of the state criminal district court in Fort Worth. Through his lawyer, Jack Beech, Burleson denies the charges but has declined further comment.

The firm has been awarded $12,000 in a civil lawsuit against Burleson. Pretrial motions were scheduled to be heard today, followed by jury selection, Garrison said.

Burleson is accused of planting a piece of computer software known as a virus in the computer system at USPA&IRA Co. two days after he was fired. A virus is a computer program, often hidden in apparently normal computer

software, that instructs the computer to change or destroy information at a given time or after a certain sequence of commands. [Trojan horse???]

USPA officials claim Burleson went into the comapny's offices one night and planted a virus in its computer records that would wipe out sales commissions records every month. The virus was discovered two days later, after it had eliminated 168,000 records.

---

computers and guns

Gary Sanders <gws%n8emr%osu-cis@pyramid.com>
7 Sep 88 02:47:32 GMT

A funny thing happened on the way to the data call..

I was sitting at home one cool evening, flipping through the channels on the TV not much on, even with cable... Every once in a while I would hear my modem dial out out the one of the many news feed sites, and hear the many machines and men calling in.. I was about ready to nod off (again), but someone was knocking rather rudely on the door.

I jump up and answer the door briefly (no pun) forgetting that I only had only my boxers on.. Well I crack the door open and it was a nice man in blue... Yes the police office stop by, ? to say hi? NO!, to collect for the policeman's ball (...), NO! Someone had called 911, in fact they called 911 three times in a row. I assured them that I didn't call but they wanted to look around and make sure I did have any dead bodies lying around so i ran in and put some pants on and unhooked the chain on the door.

They checked out the living room, then headed to the bed rooms. One bedroom is a bed room and one is a computer center, radio room (ham) and electronic scrap room (my play room). After one pulled his guns out, I got a little worried. Why did they have their guns out, I had forgotten that I had 2 UZI water guns hanging on the wall in my play room, that along with the radio, flashing lights and other terrors looking electronic gimos in the room, It must have spooked them a little.

Well they finally figured out that the guns were plastic and that I didn't have any real bombs in the room, they put away their guns.

Now they wanted to know why I called 911 three times, I told them that I had not, but they were not convinced, Well I ask them what number the call came from they said xxx.yyyy, hey that's not my number, it's zzz.aaaa then it came to me, the other number was my data line... I have no phone on the line, so it must have been the computer calling someone. Have you ever tried to convince a police officer that your computer was calling 911 by itself.. It doesn't work... They said that the dispatcher had called back but I had hung up on them, actually my modem was very polite and answered the phone and only became rude when it heard a human, then it hung on them.. Well, They left and told me (and my computer) to be careful and not dial 911 unless it's a real emergency... I say ok, and close the door.

I still wasn't sure why my system was calling 911, I didn't have 911 in the Systems file... or did I.. I check it out and found the problem. I call a site with a phone number of 891-11xx and from the logfile I had called the site 3 times a short time before the police arrived. It looked like MA Bell had take a little to long to give dialtone and the first digit was dropped. So If you want to save yourself some trouble check out your Sys files and hide your water guns...

This did happen several months ago, GUNs and ALL..
Every one in a while, like tonight I get a visit from the local PD...
I give them the story and they look around say code 4 to the dispatcher and leave..... Oh well life and data goes on...

Gary W. Sanders HAM/SWL BBS 614-457-4227
(uucp) gws@n8emr (uucp) osu-cis!n8emr!gws
(packet) N8EMR @ W8CQK (cis) 72277,1325

[This one could become a classic like the Israeli bugspray-in-the-toilet story, which resurfaced after previously appearing in an old-yarn book. We have had a variety of cases just like this in the past. But it serves as another reminder of how easily it can happen. PGN]

Automatic Call Tracing and 911 Emergency Numbers

<MCCLELLAND_G%CUBLDR@VAXF.COLORADO.EDU>
Tue, 6 Sep 88 22:41 MDT

Our local county government just worked a deal whereby for a small fee added to each customer's phone bill, the county's centralized 911 emergency switchboard would be provided with a display of all incoming phone numbers and addresses. I'm rather glad that the next time I call 911 all that information will be communicated automatically (but I hope it will still be verified orally whenever possible). However, I suppose that once we pay for the installation of the necessary technology the local telco will be able to sell it as a service to other businesses. As previous notes have suggested, there are many privacy issues to consider here but there are benefits that also need to be considered as well.

Gary McClelland

[911 ANI in LA noted by paulb@ncc1701.tti.com paulb@ttidca.TTI.COM (Paul Blumstein).]

Automatic Number ID: Bad Idea!

Andrew Klossner <andrew%frip.gwd.tek.com@RELAY.CS.NET>
Tue, 6 Sep 88 11:00:22 PDT

[This discussion has gotten pretty far from RISKS.]

"I consider an unsolicited phone call to be an invasion of my

> privacy. If you feel you have the right to call me and refuse
> to identify yourself, then I maintain I have the right to come
> to your front door and refuse to identify myself."

This is the wrong analogy. Consider a world in which, when you wonder into a shop with an idle question, the shopkeeper can, without your permission, divine your identity. There's a world of difference between "Good afternoon, what's your name? If you won't tell me, get out" and "Good afternoon, I have recorded your name and there's nothing you can do about it."

[Also remarked upon by Hugh Pritchard. PGN]

> "Anonymous is also making the assumption that the people who
> a[c]quire your number via ANI will automatically abuse the
> information. This is mostly false."

This is a Pollyanna attitude. I have worked for telephone/junk-mail solicitors (in my starving student days) who would drool at the thought of abusing this information. As an example of privacy abuse, consider Radio Shack's policy of demanding full identification, even of cash customers, for purposes of composing a mailing list.

-=- Andrew Klossner (decvax!tektronix!tekecs!andrew) [UUCP]

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 47

Thursday 8 September 1988

Contents

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

COMPASS report in RISKS 7.40

Jean-Claude Laprie <laprie@laas.laas.fr>
Thu, 8 Sep 88 08:58:07 -0200

Brian Randell forwarded me the Jon Jacky's report from COMPASS'88, and asked to comment it. These comments can be summarized by: FRIGHTENED!

I am frightened to see attendants to a congress devoted to safety issues debating on topics (the 10**-9 figure and the like) when ignoring, or wanting to ignore, their real origin and their meaning: no significant contribution to the mortality rate in industrialized countries (see the statistics from OMS, the world wealth organization).

I am frightened to see that they are confusing evaluation of a product and evaluation of a process: as a direct consequence of the former, such reliability goals cannot, by essence, be statistically assessed for a given product.

I am frightened to see specialists of safety who do not seem aware of one of the major criticisms of the Inquiry Commission after the Challenger accident, i.e. that NASA had neglected quantitative evaluations.

Jean-Claude Laprie, LAAS-CNRS, Toulouse, France.

COMPASS '88 re-revisited

<leveson@electron.LCS.MIT.EDU>
Thu, 08 Sep 88 16:01:40 -0400

I shall let Bev have the last word in this argument, especially since I cannot figure out what we are arguing about. As far as I can tell, we are in violent agreement. But he does issue a challenge to which I feel I should respond, i.e.,

>Maybe Nancy could tell us how she would reduce catastrophic failure rates to
>acceptable levels and demonstrate the achievement of such levels?

I do not believe that we should be talking about catastrophic failures at all. Catastrophic failures or accidents usually involve aspects of the environment that are not under the control of the designer of the system. Computers do not usually have catastrophic failures (unless one considers the problems of electrical shock or fire, which are usually minimal). I prefer the word used by Safety Engineers, i.e., hazards (states of the system being designed that could lead to accidents or catastrophic failures given certain environmental conditions). As a component of a larger, potentially hazardous system, computer software can certainly contribute to the system hazards and thus has some hazardous (but not necessarily catastrophic) failure modes. Considering only catastrophic failures limits the problem too much.

So how can software-related hazards be eliminated or reduced? The practice of System Safety Engineering provides some direction. Details will be in my book (coming out next year from Addison-Wesley) and my survey article also describes this (in less detail) but briefly: The first step is to identify the hazards of the system being designed. System safety engineers call this a Preliminary Hazard Analysis. This part of the process often involves knowledge of previous systems and accidents and requires more creativity for one-of-a-kind or first-time systems. However, even these can be analyzed using information about general types of hazards such as electrical shock, chemical effects, or radioactivity exposure. Analysis techniques, e.g., Failure Modes and Effects Analysis (although this is usually used more often for reliability analysis than for safety analysis) and Fault Tree Analysis, are used to determine plausible events that could create hazards. Design procedures are then used to try to eliminate or minimize these hazards by either preventing the precipitating events from occurring (i.e., designing them out), minimizing the probability of their occurrence, or minimizing their chance of leading to the hazard. Bev should note, here, that probability is involved and thus measurement or estimation. But the key is that measurement alone leads us to a fatalistic yes/no choice whereas measurement combined with design allows us some further options in attempting to find designs that have acceptable risk.

My books and reference materials are currently somewhere over the state of Kansas, so system safety engineers may need to correct some of the

following. But the general goal of system safety design is to eliminate single events that can lead to hazards and to minimize the probability of multiple events or sequences of events leading to a hazard. Thus the desire of the engineer with whom I spoke to get a number for the event of a particular type of software behavior. Since I did not know of any way that he could obtain this number with the amount of certainly he and I felt were necessary when a nuclear plant meltdown was involved, I thought it best for him to use 1.0 for this probability and design around this event (i.e., design the system so that the event would not cause a hazard).

Engineers have various ways of eliminating hazardous events (what I referred to sloppily in my previous message as "catastrophic failure modes) from systems or minimizing their probability of occurrence. For example, the hazard of electrical shock can be eliminated by designing a purely mechanical system. This is a rather extreme solution, however, and often unacceptable. Another less extreme solution is to use interlocks to prevent certain events or to ensure proper sequencing of events. For example, a door over a high voltage area is often used to protect against accidents. The door can be designed so that when it is open (and the high voltage equipment exposed), the circuit is broken.

Note that the use of interlocks are often simply a matter of designing the system so that multiple independent failures are required for hazards to arise: The interlocks themselves may fail. Assuming that common point failure modes (which engineers have techniques for identifying) are eliminated or minimized, then risk will be reduced. Probabilistic Risk Assessment (PRA) can be used to determine if the risk is acceptable, but even for non-computerized systems PRA is controversial and criticized as inexact. The most accepted use of PRA is for comparison of alternative designs. PRA has been primarily used in the assessment of the safety of nuclear power plants, and there is at least one interesting critique of this use that has been published by the Union of Concerned Scientists.

Several accidents I have heard about have occurred when computer subsystems replaced electro/mechanical subsystems without replacing the interlocks that maintained adequate levels of risk. The same mechanical interlocks or back-up systems can be included to protect against computer errors (probably the safest since we can assess the risk involved fairly accurately using historical information) and/or various kinds of interlocks can be included in the software. In this case, software reliability assessment is involved since the reliability of the software interlocks will be crucial. Since these software interlocks are often quite simple and limited in required functionality, I believe (and I realize that others might not agree with me), high reliability MAY be achievable by using sophisticated software engineering techniques including, perhaps, formal methods. I might be willing to accept subjective assessments of risk here if the software is simple enough whereas Bev might not. If subjective types of assessment (including the use of formal methods) is not acceptable, then we may be forced to rely on mechanical back-ups, probably in addition to the software interlocks (again, the goal is to require as many independent failures as possible for a hazard to occur). [Note that some hazards are unavoidable, and the design goal then becomes minimizing the amount of time in the hazardous state.] Probably neither Bev nor I would agree to the use of another computer as the backup, even if the

code is written by a separate group of people because of the problem of eliminating common failure modes, i.e., non-independent failures (e.g., the same software requirements specification). The point is that this does not mean that the reliability of the entire software system (which may be quite large and complex) needs to be ultra-high, only the smaller safety-critical parts. If the software is designed, as is common with software engineers who do not know enough about safety, so that it is ALL potentially safety-critical, then the problem becomes quite overwhelming, and Bev and I (and others) find ourselves with planes or other devices that we do not feel safe using.

Hopefully, I have not made too many mistakes in this brief summary of System Safety Engineering. If I have, I am sure that the other Risks readers will correct me :-).

Nancy

Calling number delivery

John (J.) McHarry <MCHARRY@BNR.CA>
8 Sep 88 13:41:00 EDT

The telephone feature of delivering the calling number to the terminating line is part of a group of features called 'CLASS', although there are other ways it could be done in certain special cases. There are a number of Bellcore publications that describe it in some detail. Among these are TR-TSY-000031 on the basic feature, (TA) 000030 on the signalling between office and customer terminal, 000391 on the feature to block delivery of the calling number, 000218 on selective call reject, and (TA) 000220, also related to selective call reject. TAs are an early version of TRs. If you don't find one in a reference,look for the other. There are several other TRs that relate to these features, but this list should sate most of us.

Calling number delivery, selective call reject, and calling number delivery blocking are all involved with the 'Signalling System 7' which is just beginning to be deployed amongst local exchanges, although some of the long distance carriers are much farther along. Among other advantages, SS7 enables the transfer of much more information between network nodes than was previously generally available. This should allow the introduction of many new network services in the near future. On the other hand, CLASS and calling number delivery in particular will not likely become common until large areas are cut over to SS7, since otherwise they would not work much of the time. (Only within the local switching office, or among those that had already implemented SS7)

It looks to me like a subscriber to calling number delivery gets telemetry intended to allow display of the number calling concurrently with ringing. I suppose proper customer premise equipment could pick this off and feed it into a computer or use it to determine what to do with the call, eg. route to an answering machine only if not long distance. If the number isn't available, as would be the case if the originating and terminating offices were not linked by SS7, the telemetry sends ten 0s. If the number is available but the originator is blocking delivery, it sends ten 1s.

Calling number delivery blocking is itself a CLASS feature that can be set on by a service order or, depending upon the tariffed offering, turned on or off on a per call basis. How it is offered, if at all, is up to the local telco and PUC. The TR makes it look to me like it is not available to party line subscribers. I think there is a technical reason for this.

Selective call reject allows the subscriber to set up a list of up to N directory numbers (N might be on the order of 6 to 24) that would be sent to 'treatment' instead of ringing the subscriber's phone. A caller using blocking could be put on this list after one call by using a control that says, in effect, add the last caller to my list, but that number could not be read from the list by the subscriber. It doesn't look to me like the blocking code itself can be put on the list; maybe somebody else knows a way or has tried it. Call reject can be turned on or off also, and can be maintained from either a DTMF or dial phone.

There might be something here for everybody. If I can block delivery of my number and Mr. Townson can send me to treatment we would be almost as well off as with Internet addressing from Bitnet to Portal.

The foregoing opinions and interpretations are mine, not my employer's. My interpretations of the referenced documents are based on a cursory reading. They probably contain some errors.

John McHarry McHarry%BNR.CA.Bitnet@wiscvm.wisc.edu

More on Automatic Call Tracing and 911 Emergency Numbers

Robin j. Herbison <LADY%APLVM.BITNET@CUNYVM.CUNY.EDU>
Thu, 08 Sep 88 16:47:11 EDT

A co-worker of mine called the Police last year to report a burglar alarm in his neighborhood which was going off. (He lives in Baltimore County, Maryland.) The dispatcher received the phone number, his name and an address automatically.

The 911 dispatcher read back the address that was displayed. It was where they had lived two(2!) years previously. When they moved, they kept the old phone number and gave the phone company his the address. Unfortunately, the change of address was not passed on to 911.

Although it would be nice to have 911 come if you were in trouble and and could only lift the phone, I would like them to arrive at the Current address. (I know the people who live at my old address do not know my current address, although I assume they have a current phone phone book. Since I am listed, They could direct the police to my home.)

Quite a waste of time, esp. in an emergency.

ANI on 911 calls

<forags@violet.Berkeley.EDU>
Thu, 8 Sep 88 08:38:42 PDT

The Alameda County phone book has a privacy notice right below the 911 number which warns callers about ANI and advises them to use the regular 7-digit number if they don't want their number displayed on the dispatcher's console.
-Al Stangenberger

Another ANI scam (Re: RISKS-7.45)

Brent <brent%itm@gatech.edu>
8 Sep 88 13:15:59 GMT

Here's another scam for ANI. Set up a free phone service: time and weather, point spread predictions, sports score line, Dow Jones business news brief. It's just a taped message someone can call into. Now set up a PC to capture the ANI information on people who call. Take the diskette of phone numbers to a service that offers CNA (customer name and address) and presto! You have yet another profiled mailing list ready to be sold to hungry marketers of sports equipment, business journals, etc. Where'd they get MY name? you ask. You'll never know.

ANI is going to be big business. Just north of Atlanta is one of the new AT&T regional billing centers. Their goal is to fully integrate ANI with their customer inquiry department. So when you call 1-800 whatever, the AT&T rep will answer "Good morning Mr. Jones, how's the weather in Macon? I'll bet you're calling about that collect call to Bogota." They'll have your name, address, and billing info on the screen in front of them as they answer your call.

Hmmm... try forwarding your calls to AT&T. What will happen?

Brent Laminack (gatech!itm!brent)

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 48

Friday 9 September 1988

Contents

- COMPASS 88
  - Bev Littlewood
- Safety Engineering
  - WHMurray
- Technical naivete revealed by responses to VINCENNES incident
  - Jon Jacky
- Vincennes: Rules of engagement violated by AI heuristic?
  - Clifford Johnson
- ANI Response
  - Patrick A. Townson
- Proposed ANI Enhancement
  - Rob Boudrie
- ANI blocking defeats purpose
  - Bob Philhower
- Credit Card Loss Woes
  - Clay Jackson
- Info on RISKS (comp.risks)

COMPASS 88

B.Littlewood <sd396@CITY.AC.UK>
9 Sep 1988 16:05:35-WET DST

Nancy says she is going to let me have the last word in this saga. Unfortunately, it is not clear whether my last comments represented this 'last word': after all, Nancy only responded with a mere two page reply - this probably doesn't count!

She is right that we agree on more things than we disagree. But it is the disagreements that are much more interesting to discuss. So here goes once more . . .

I ended my previous note by asking Nancy how she would "reduce catastrophic failure rates to acceptable levels and demonstrate the achievement of such

levels". Her reply falls far short of answering this question. Indeed, it is largely a recital of elementary 'good practice' (in England we say "teaching your granny to suck eggs").

Let me spell it out again. First of all, by the phrase "catastrophic failure rate" (to which Nancy takes exception) I meant merely the rate at which her "catastrophic failure modes" show themselves in operational use. It is this rate determines in a formal way how we can talk about safety in a quantitative way for some systems (it is not appropriate for all systems).

Even quite unsophisticated members of society can appreciate concepts like this when they are presented appropriately, so it represents part of a fromal-ism which also has intuitive appeal. A safe system is one that does certain specified nasty things SUFFICIENTLY INFREQUENTLY.

In my earlier note I agreed with Nancy that we only want "an acceptable level of safety". We seem to be in dispute about what this means, how we can get it, and how we can assure ourselves that we got it. I think there are three stages to this:

1. We need to decide what are the nasty undesirable events (e.g loss of life, or loss of airframe, in civil aviation).

2. We need to decide how frequently we can tolerate these events (e.g. 10**-7 per hour for some airliner events)

3. We need ways of ACHIEVING such an "acceptable level of safety", and of DEMONSTRATING ITS ACHIEVEMENT in each particular context.

As I understand it, Nancy does not wish to define "acceptable level of safety" in a way akin to 1 and 2. I remain puzzled, therefore, as to what she does mean by such a phrase. It is difficult, therefore, to know whether her claims to be able to achieve an "acceptable level of safety" by "other solutions" should be given any credence.

Certainly, the methodology in her latest note (whilst being good practice and probably necessary) falls woefully short of satisfying 3 above. I am prepared to accept that use of these techniques is better than not using them: they are likely to improve safety/reliability. Knowing that they will increase safety, however, is far short of knowing that their use will be sufficient to achieve a particular goal of "acceptable safety" as defined in 1 and 2. They do not assist at all in telling us what level has been achieved.

No, it seems to me that Nancy is claiming that certain "good practice" is a solution to our problems. I agree that her "good practice" is a lot better than most ACTUAL practice, but I remain sceptical about its efficacy.

In case this sounds merely academic (must stop using that pejoratively), a cynic for civil airliners is even worse than Nancy's suggestions. As I understand, the A320 fly-by-wire was certificated against RTCA Do178A. This appears to have no definition of "acceptable level of safety" and, worse, lays down only very minimal "good practice". To give them their due, Airbus Industrie seem to have been sufficiently embarassed by this state of affairs that they got embroiled in 10**-9 and all that. The system is certificated in Europe,

the thing is carrying passengers, yet, I believe, it cannot be asserted in any scientifcally meaningful way that it has an "acceptable level of safety".

This brings me to Peter Neumann's elucidation of John Cullyer's original remarks at COMPASS. Now that they are clarified they seem ever more appalling! Certification seems to merely mean that a certain formal test (e.g. conformance to Do178A procedures) has been passed. This test might even relate only to "good practice", I suppose, and need not involve any evaluation of product behaviour (as is the case for Do178A). Yet Cullyer suggests that such a certification should be used instead of evaluation of achieved safety/ reliability.

It is clear that certification of this kind will not assure us that a particular product will be sufficiently safe. Could John tell us how he would go about getting such an assurance?

Finally, a slightly mischievous plug for the probabilistic/statistical approach. I suppose one of the most extreme problems which gives rise to the difficulty of the assurance problem lies in the correctness (or not) of the specification. And one of the most difficult problems there concern omissions from the specification: things that should have been thought of, but weren't. I think it is clear that none of the techniques suggested by John Cullyer or Nancy Leveson can attempt to quantify the inpact of such omissions on system reliability (although they may help to identify some of them). Only the statist for a certain time without revealing the effects of such omissions, we can estimate their contribution to its unreliability. This if the flip side of the excellent work of Doug Miller described at the COMPASS meeting. OF COURSE, this reliability (Miller'spoint). OF COURSE, it occurs too late in the life cycle (we want the assurance at a time when we can do something about impending problems). Even so, I don't think any of the other approaches do anything about evaluation here.

Bev Littlewood
Centre for Software Reliability
London EC1V 0HB

PS I'm out next week. Since I'm betting Nancy can't resist breaking her uncharacteristic vow of silence, a reply might take some time. A relief to everyone, no doubt . . .

Safety Engineering

<WHMurray@DOCKMASTER.ARPA>
Fri, 9 Sep 88 08:54 EDT

Nancy Levenson's latest was a breath of fresh air. It put some rationality into what was becoming a silly discussion.

In it she comments:

>..again, the goal is to require as many independent failures as
>possible for a hazard to occur.

Before anyone gets too carried away with that strategy, I would simply point out that their are limits to its effectiveness. There is a point at which adding additional safeguards and redundancies begins to add complexity and failure modes of their own. The great northeastern blackouts are examples of what happens when this strategy is carried too far.

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

Technical naivete revealed by responses to VINCENNES incident

Jon Jacky <jon@june.cs.washington.edu>
Fri, 09 Sep 88 09:36:54 PDT

Last night (Thurs. Sept 8, 1988) I heard another story about the VINCENNES /Iran Air incident on the NPR radio news program, "All Things Considered." The occasion was a presentation by the Navy to the Senate Armed Services Committee. No new information was presented, but several comments by the participants and by the commentators was quite revealing of attitudes about computing among lay people. First there was a tape of a Navy official (whose name I did not catch) telling the Committee (this is a close paraphrase; I took notes immediately after hearing the story):

"We have determined that the Aegis radars and computers functioned correctly and that the misidentification of an Airbus airliner as an F-14 was due to human error induced by combat stress. ... The operator interpreted a display indicating the Airbus was at 12,000 feet and flying level as indicating it was
at 7,500 feet and descending toward the ship ... However, we are looking at the user interface - what we show on the displays - there may be some room for improvement there, to make it even more user-friendly than it is now..."

The interesting bit in this passage is calling the mininterpretation of the display "operator error" rather than "design error."

Even more interesting was an interview with retired Navy Commander James Meachum (I'm unsure of the spelling of the last name). Meachum is now the defense reporter for THE ECONOMIST, a highly regarded British weekly news magazine. The interviewer asked if Meachum agreed with the "human error/ combat stress" explanation for the incident. Meachum replied:

"There's an aircraft out there, what's its heading and speed? That's a very straightforward problem and I can't believe the system could have gotten that wrong ... It's been very thoroughly tested. It is possible that some other part of the system might have failed, but I doubt it..."

This statement reveals two very common misconceptions about computer systems that I encounter all the time. The first is, "if it seems simple to me, then the computer must get it right." The other is, "if the system passes a test, then it will also perform correctly on other cases that seem similar to me."

Both of these attitudes are simply anthropomorphic superstitions, but they are very deeply seated in lay people. I have found myself trying to convince my colleagues at work that results from a program that I wrote were probably in error and should be investigated, while they maintain the results "must be right" because "we tested a case just like that."

The effect of these misconceptions is to discourage thorough investigations of possible problems. I now doubt the frequently heard assertion that the Vincennes actually did correctly identify the altitude and heading of the Airbus. This assertion is supposed to have been proved by examining "files" or "tapes" from the Vincennes. Does anyone know if these records include videotapes of what was actually shown on the displays at the time of the incident? If not, why do they think they know what the operator saw? Or, do the tapes actually capture data from some point nearer the signal source, "upstream" from the displays? Have the investigators assumed that the displays "certainly must have" shown images consistent with the data on the tapes? I have always thought the operator's report of the altitude and heading sounded a bit too specific to explain away as the result of stress.

Why is it that people "just can't believe" that the computers might have scrambled this up, but can easily believe that the operators did scramble it up?

- Jonathan Jacky, University of Washington

Vincennes: Rules of engagement violated by AI heuristic?

"Clifford Johnson" <GA.CJJ@Forsythe.Stanford.EDU>
Fri, 9 Sep 88 09:28:27 PDT

> "Not transmitting proper IFF will be taken into account"
> AND
> "Not remaining in proper airways will be taken into account"
> IMPLIES
> "Not responding to warnings will be taken into account"
> doesn't hold.

What I said does hold, if the declaration is to be given a reasonable construction. Note my use of the word "seems":

> So it seems a post-facto revision of the rules of engagement to assert that failure to respond to warnings is per se sufficient cause for deadly force *until proven otherwise.*

The U.S. declaration that Captains would take into account the fact that commercial planes might behave *very* irregularly, a fortiori implies they would strongly credit that such a plane behaving only *slightly* irregularly (and ignoring or delaying response to warnings was in fact usual) would be construed as commercial. Thus, the rule that conclusively defined every plane taking off from Bandas Abas as hostile until *proven* otherwise squelches this promised caution.

True, there was no declaration that the U.S. would not shoot down a plane thought probably or possibly commercial, but if this were not the case, then the declaration would be purposeless, and misleading at best.

ANI Response

<sun!portal!cup.portal.com!Patrick_A_Townson@unix.SRI.COM>
Thu Sep 8 17:48:01 1988

Recent correspondents in RISKS have challenged my comment 'no good reason to conceal telephone number'. Examples of 'good reasons' include calls to hot lines, counseling services, police officials, and others.

Here in Illinois, the law which enabled 911 Service, and required its implementation in all communities in the state also required that every Police Department have a seven digit administrative telephone number to receive non-emergency calls and calls made 'in confidence' by the caller. The Chicago Police Department & Fire Department can be reached through the main centrex number for the City of Chicago Offices: 312 - PIG - 4000. To reach individual police officers, etc, just dial PIG and the desired 4 digit extension. And not that I would expect everyone to know it, but you *can* override ANI on 911 calls in most cases by knowing which *seven digit number* 911 is translated into by your local phone office. Here in Chicago it is (or was) 312-787-0000. Calling that number reaches 'Chicago Emergency' just as surely as 911, and with only a blank screen for the dispatcher to look at in return. Apparently when you dial 911, your central office translates it into a seven digit number and sends encoded information containing *your number, and address* to the dispatcher when it puts the call through to the ACD (automatic call distributor) at the police station.

Since posting my original article a couple days ago, I have researched this a bit further and find the general thinking among folks I have contacted at Illinois Bell is that there will be specific exemptions in the tariff for calls to crisis lines, counseling services and similar where those groups will NOT be permitted to subscribe to ANI signaling service. And those exceptions mentioned by the writers here do make good sense.

As for stockbrokers and others who are likely to try and make a hard sell, what do you do now when these people routinely ask for your phone number in the process of taking your order/giving information? Refuse to give it? Give a false number? Whatever happened to your spines? Just say NO to the broker. Just say no to the Operator Who Is Standing By To Take Your Call Now....

Patrick Townson

Proposed ANI Enhancement

<ROB.B%te-cad.prime.com@RELAY.CS.NET>
09 Sep 88 00:30:10 EDT

If digital data is going to be transmitted with phone calls, why not add a "classification code" (perhaps 3 digits) which may optionally be sent by the caller. Add to this legislation which requires all human telephone solicitors to send a digital class code of "001" with their calls, and all tape playing sales machine generated calls to carry a class code of "002". The phone company could then offer a "class selection" service whereby the subscriber could make his phone inaccessible to selected classes of calls.

This is not without (manual) precedent. All companies using tape playing sales machines within Massachusetts are required by law to check the numbers they will call against a phone company maintained list of subscribers who have requested not to be bothered by these machines. This list must really work - I was on such a list and have only recently begun to receive that form of harrassment, commencing right after my area code was changed from 617 to 508.

Rob Boudrie

ANI blocking defeats purpose

Bob Philhower <philhowr@unix.cie.rpi.edu>
Fri, 9 Sep 88 10:09:55 EDT

It is naive to think that an ANI system with a blocking feature (i.e. you prepend the number you dial with something like *21 to prevent your own phone number from being available to the party you call) would have any effects on those who abuse the anonymity of the current system. Anyone that concerned about his/her privacy would purchase a device to sit on the phone line and recognize the first dialed number, delay it, and send *21 before it. (If these don't appear immediately, I would certainly market them myself.)

Credit Card Loss Woes

<microsof!clayj@beaver.cs.washington.edu>
Fri Sep 9 08:49:04 1988

Here's yet another potential problem when one loses a credit card:

Last Monday (9/5) I left my cash machine "Access Card" hanging in an ATM. Fortunately, this particular machine (a Fujitsu) is smart enough to capture cards left in it by forgetful users.

The real problems started when I discovered the card missing about 1900 on Tuesday (9/6). Since I had no idea where I might have left it, I decided to be safe, and called the phone number given on the back of my wife's card for reporting lost or stolen cards. I was greeted at that number by a recording, which informed me that the issuing bank's offices were closed for the day, and gave me ANOTHER 800 number to call to report a missing/stolen card. I called the second number, and a human answered "National Credit Center", and took down the expected information about my lost card, including my work and home phone numbers, address, and mother's maiden name. She did seem a bit comfused as to the type of card I was reporting as missing, and had no idea if my wife's Access Card (with the same account number) would be blocked as a result of this action.

On Wednesday, during business hours (about 1300, or 18 hours AFTER I reported the card missing), I called the issuing bank's card office, and checked to see if they had in fact received the report. They had NOT yet received the report, and had no other indication that the card was missing. I gave them another report, and they "blocked" the card. On a hunch, I called the branch (of the same bank) where the Cash Machine I had last used was located, and they told me "Yes, the machine did capture your card, and we destroyed it, since we were unable to contact you". I have no idea why they were "unable to contact" me, since they have on file (I verified them) there at the branch (it's our "home" branch) correct phone numbers for me, both at work and at home, we have an answering machine at home, and my wife was home all day on both Tuesday and Wednesday! It also amazes me that the Card Dept of the same bank had NO IDEA that the card had in fact been recovered on Tuesday, OVER 24 hours before I called (the bank) to report the card missing.

The last, and worst, part is that on Thursday, in the space of about 3 hours, we received 4 separate phone calls (3 at home and one at work) from "Credit Card Protection" services. They ALL began with some variation on the theme "We understand you've just lost a credit card" (two of them knew the NAME of the card we had lost, one just said "credit card" and one said "MasterCard). Obviously, SOME organization (either the bank or the "National Credit Center" had, in less than 48 hours, given (or sold) our name, phone number, and the fact that we had lost some sort of card to not one, but FOUR separate companies.

To the bank's credit, when I called their "Corporate Affairs Officer", he was almost as unhappy as I was, and has promised me a full investigation and return phone call. He assured me that the selling of that information was "against corporate policy, and possibly state or federal laws". I'll post a followup to this forum with the results of his findings.

Clay Jackson, Microsoft, Redmond, WA {...microsoft!clayj}

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 49

Sunday 11 September 1988

Contents

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

Firmware bugs in Dutch gambling machines

P. Knoppers <knop%dutesta%mcvax@uunet.UU.NET>
Sat, 10 Sep 88 17:21:03 -0200

In the Netherlands it is legal to exploit gambling machines if these are approved by a government-operated test institution.

There is currently an approved machine in use that has a rather severe problem in its firmware. This fault can be exploited by malicious players. I will not reveal which machine type has the bug, there may even be several models that have it.

The trick is as follows:
Use the machine until you have won a substantial price (call this price 1).
Pull the power plug BEFORE the machine has started to pay out.
Re-insert the power plug.
The machine will self-test and pay out the pending price 1.
On the next price that you win (no matter how small) the machine
pays the amount of price 1.

The use of this trick can empty the coin buffer of the machine within
one hour.

It appears that a system that was designed to protect the players from
financial losses in case of a power failure introduced a risk.
Makes me wonder what measures are built in ATMs to protect customers
in case of a power failure during a transaction...

P. Knoppers - knop@dutesta.UUCP
Delft Univ. of Technology, Faculty of Electrical Engineering, The Netherlands.

Soviets See Little Hope of Controlling Spacecraft

Gary Kremen (The Arb) <89.KREMEN@GSB-HOW.Stanford.EDU>
Sat 10 Sep 88 15:22:49-PDT

According to today's (Saturday, September 10, 1988) New York Times, the
Soviets lost their Phobos I spacecraft after it tumbled in orbit and the
solar cells lost power. The tumbling was caused when a ground controller
gave it an improper command.

This has to one of the most expensive system mistakes ever.

Gary Kremen, Stanford Graduate School of Business

[Several people reported on radio items that attributed the problem to a console operator's single keystroke in error, which it was speculated might have triggered the Mars probe's self-destruct signal. After the command was sent, contact with the probe was lost completely. PGN]

Disinterest in disaster is not based on probability estimates.

"Clifford Johnson" <GA.CJJ@Forsythe.Stanford.EDU>
Sat, 10 Sep 88 18:18:00 PDT

A recent contributor noted disinterest is a planned conference
on disasters in Chicago. Another noted:

> John Cullyer of the British Royal Signals and Radar Establishment ... said,
> "Let's throw out the 10 ** -9" - and many of the audience responded with
> enthusiastic applause. Someone asked if he would accept a failure
> probability of only 10 ** -4 or 10 ** -5 for nuclear weapons safety. He
> responded, "In the weapons area there should be no room for probability. If

> something is unthinkable, don't let it happen. You either certify it or you
> don't - one or zero."

Three months ago I was set for a 2-hour interview/call-in program on the San Francisco CBS radio station. My topic was the probability of computer-related error causing accidental nuclear Armageddon, which even conservative authorities (e.g. Hudson Institute) estimate to have a probability of the order of 10**-3 per year. I reckon it's higher, and can argue the point.

On arrival, I found my time reduced to one and a half hours because of a change in the computerized California lottery which provided for a bigger multi-million $ jackpot at even longer odds. This topic was inserted as a first interview/call-in feature, for half an hour before me. The odds of winning the jackpot per ticket must be of the order of 10**-8. Even buying a hundred tickets per year doesn't get the odds above 10**-6 per year.

Maybe you can guess the rest. The station had a screen displaying the status of the five incoming phone lines. They were packed for the lottery call-in. For example, animated callers complained that South California got more prizes than the North, and the lottery official patiently responded that the prizes were in fair proportion to money spent. Etc. Clearly, the lowering of the odds of success (which the official never quantified) was of scant concern to callers agog at visions of the higher jackpot. The lottery debate was extended for a further half hour. I didn't mind: one hour is more than enough for my message.

In the first 25 minutes of my call-in interview, there was not a single caller. There were only three in the entire hour.

What a Ticonderoga Combat System "records"

John Allred <jallred@VAX.BBN.COM>
Fri, 9 Sep 88 17:36:05 EDT

Jonathan Jacky, University of Washington, asks:
>The effect of these misconceptions is to discourage thorough investigations
>of possible problems. I now doubt the frequently heard assertion that
>the Vincennes actually did correctly identify the altitude and heading of
>the Airbus...

First off, my credentials on this subject: I worked on the Combat System of a Spruance Class Destroyer, a direct predecessor of the Vincennes (and other Ticonderoga Class Cruisers). Indeed, a "Tico" has the same hull as a Spruance. Add that nifty phased array radar (SPY-1), lots of missiles, and an enhanced Combat System (5 tactical data computer (AN-UYK7), versus 2 on a Spruance), and you get a Tico. The Combat System on the Tico is also known as AEGIS.

The Combat System records, in real time and on magnetic tape, the symbology seen by the radar operators anytime the "program" is up. During training, it was common to "play back" a canned scenario to exercise the troops and equipment. So, when the Investigation Officer's report says, "AEGIS reported Iran Air 655 as ascending", the Investigation Team probably replayed the tapes

of the incident, and saw a display reporting Iran Air 655's status *AS THE CREW SAW IT*.

John Allred, BBN Systems and Technologies, Inc.

High-tech toilets

Robert Dorsett <juniper!mentat@emx.utexas.edu>
Sat, 10 Sep 88 19:17:27 edt

Pages 132-136 of the 9/3/88 issue of Flight International has a summary of the first six months of A320 service with British Airways (3 airplanes) and Air France (2 airplanes). Mulhouse-Habsheim crash not withstanding, both airlines claim a dispatch rate of approximately 97%. Some highlights from the article:

1. Problems with air conditioning packs, which have resulted in BA restricting fan output to 80% of suggested maximum. This is listed as a supplier problem.

2. The FADEC (full-authority digital engine control, a fancy term for a computer-controlled fuel metering system) has been reliable, although Air France claimed frequent replacements in the first few weeks of service.

3. The computer-controlled cabin public address and lighting system does not work very well. Both airlines are disgusted at the sloppyness of it. Again, it is listed as a supplier problem.

4. The toilets don't work very well (see excerpt below).

5. There was mention of in-flight failures of the primary guidance system, but the backup systems worked as advertised.

6. There have been software modifications of the "flight management and guidance computer, fuel quantity indications computer, cargo compartment ventilation computer, avionics equipment ventilation computer, window heat computer, and bleed monitoring computer." (One wonders when they will replace a simple on/off switch with a computer). The modifications were required when some computers shut down after the power sources for the mains was switched from the APU to the engine generators.

7. 95% of all system faults have occurred after engine startup, before the airplane got in the air. En route failures are rare.

On the plus side, BA claims that the centralized fault display system, which is a CRT and possibly a printer, intended for use by maintenance personnel, has been quite successful in detecting faulty items and systems, improving maintenance time considerably. They have encountered the occasional unintelligible message, though. They look forward to incorporating the system with a communications package to let it automatically call maintenance bases to let maintenance personnel "get ready" for a quick repair job on the airplane when it arrives. The CFDS is based on the late 70's AIDS (Airborne Indicated Data System), tested with mixed results on the 747, and later on the 757/767.

The device keeps track of data which is not normally of operational significance. The data can then be offloaded, catalogued, analyzed, etc. Apparently Airbus has incorporated an expert system to form the latest version.

It should be observed that something Steve Philipson said, about the Airbus being very much an "experimental aircraft," holds weight, even though the concentration of problems has shifted. Airbus is said to be keeping a full staff of engineers on site at Air France and British Airways maintenance bases. In addition, each airplane is carrying a set of computer "spares" (spares for what, the article doesn't mention) in the event of failure. The article does not indicate how long this arrangement is going to last.

Now, about the toilets... (excerpted without permission, but let's say it's for the purposes of review)

"The main concern about the A320 has been that so many functions are 'computer-controlled,' and that this could lead to unforeseen problems. The use of the word 'computer' can be misleading, in fact, because many of the devices referred to as computers are little more than digitally controlled switches--like the window heat computer, whose software has now been spike-vaccinated.

"The whole subject comes firmly down to earth in the Air France A320's, where the high-tech vacuum toilet system chosen by that airline (but not by BA) has suffered shutdown because of glitches caused by electrical transients. Aircraft have been grounded by this problem from time to time. You can get an aircraft airborne safely without working toilets, but it is unwise to try to get any passengers airborne under those conditions.

"Air France chose the vacuum toilet system for its single-point drainage and the flexibility to move a toilet quickly for a short-notice cabin reconfiguration. However, its A320's have been subject to four different types of toilet system malvunction: toilet overflow, toilet shutdown, system shutodwn, and straightforward toilet drain blockage. The latter may be a matter of wastepipe diameter, though not everyone agrees on that. It has worked on other aircraft.

"Airbus, in its produce support department's technical review of Air France's A320 toilets problem, devotes a page to the subject, with a chart designating specific problems followed by progress towards rectification. The toilet overflow was caused by a rinse-valve which was sticking open. The temporary remedy is a valve modification, but a redesigned valve is on the way. The individual toilet shutdown and the whole-system shutdown have been caused by electrical transients which affected the digital flush control units (FCU--the minicomputer activated by the button which the user pushes to flush the toilet) and the vacuum system controller (VSC--another microprocessor). The printed circuit boards for the FCU and VSC were under study for modification, and new software should have been supplied for them both by now. As for the drain blockage, Airbus and the system vendors were examining the suction unit in thorough system tests, and hoped to have a result by the end of August."

It should be added that the A320's fuel efficiency is listed at 40% better than that of the 727. Overall efficiency has yet to be determined. The order book stands at either 428 aircraft ("Flight") or 350 aircraft ("Aviation Week"). The word "computer" and the term "high-tech" is very clearly selling the airplane. Flight lists eleven A320's currently in service.

Robert Dorsett University of Texas at Austin
Organization: Austin UNIX Users' Group, Austin, TX

ANI/911 Misconceptions

Dave Robbins <dcr0%uranus@gte.com>
Fri, 9 Sep 88 11:00:46 EDT

It may be worthwhile to clear up some small misconceptions that have been appearing in the Automatic Number ID discussion. More than one correspondent has equated the 911 automatic identification with the calling-number identification just now becoming available to local subscribers. In fact, the two are entirely different features -- implemented differently and having nothing little more than their general behavior in common. In particular:

1) "Enhanced 911" (as it is properly called -- regular 911 is nothing more than an easy-to-remember and quick-to-dial number; it does not identify the caller) is implemented by essentially the same mechanism as ANI for toll calls. In both cases, the calling number is sent out over a trunk line, not over a local subscriber loop. As far as I know, this type of calling number identification has never been made available to businesses, as one correspondent suggested it might.

2) Calling-number-identification (there is a marketing name for this, but I forget it offhand) is a feature available only from the newest ESS and competing switches, and requires special equipment on the subscriber's premises as well as special hardware and software on the switch (and of course more money from the subscriber :-). As far as I know, each subscriber has the option of specifying -- permanently -- whether or not his number will be disclosed to others via this feature; the default value for this option would reflect the subscriber's current selection of a published or non-published number. In addition, as mentioned by some correspondents, on a given call a subscriber may choose -- via a dialed prefix -- whether or not to allow the display of his number on the called phone.

Caveat: although I do work for a "phone company" my knowledge of the above is not necessarily 100% accurate or up-to-date, since I have not been directly involved with the gory details of these particular technologies.

RISKS relevance? My concern is twofold:

1) Confusion between two apparently similar but in fact considerably different systems can result in the risks of the one being *assumed*

to be identical to the risks of the other, when in fact this is not the case. In the example at hand, there is no assumption of a right of privacy when calling 911, but there is an assumption of such a right when calling everyone else. These assumptions are made by the respective systems, reflecting what is presumed to be the same assumptions made by the general public. Viewing one system as though it were the other changes the perceived risks.

2) Much of the discussion in RISKS on this topic (and others, of course) is based upon incomplete information and therefore incorrect assumptions about the technology involved. This is, I realize, a general problem, and perhaps unavoidable. However, when discussing the risks of technology, computer or otherwise, we need to take particular care to base the discussion upon the facts, so that we can discuss the risks of the system as it actually is implemented.

Dave Robbins, GTE Laboratories Incorporated, 40 Sylvan Rd., Waltham, MA 02254

Re: Display of telephone numbers on receiving party's phone

<attcan!utzoo!henry@uunet.UU.NET>
Sat, 10 Sep 88 00:25:03 EDT

People are missing an important issue here: there is no one-to-one correlation between the number you are calling from and your identity. In particular, it is quite possible to have situations in which a call is not anonymous -- in the sense that the caller has no intent to hide his identity -- but does not want his location known. This is also the underlying problem behind having phone solicitors calling from uncallable numbers: what you want is identity and contact information, not just the number used to make the call.

Henry Spencer at U of Toronto Zoology

Social content of computer games

<postpischil%being.DEC@decwrl.dec.com>
Thu, 8 Sep 88 08:38:56 PDT

Ed Nilges writes of the decline of the social and moral content of games. But he examines only a small number of games. Consider chess, that game which allows players to act the roles of strategists without teaching them either the misery of dying under a horse's hooves or the evils of a caste system. The tactics are beautiful; the content is vile. Clearly it is not technology encouraging any moral or social decline here. Perhaps parents should picket chess clubs.

Nilges' examples are not representative of the games. The top character of Punch-Out is black. Metroid features a character in a suit of high-tech armor. If the player has done well enough at the end of the game, the character will take her helmet off. Many games take the form of a quest to defeat evil -- Ghosts 'N Goblins, Legend of Zelda, Solomon's Key, Super Mario Brothers.

Popeye is supportive of the underdog. Games like Gauntlet or Mario Brothers reward teamwork. Penguin Land requires that one learn to take care with a fragile egg. There is a wide variety to be found in games, so one could find examples of many things by concentrating on only certain features.

Computers have made games flashier, more fun, faster, and more visible, but they have not changed the social content.

Eric Postpischil

Social content of video games

<attcan!utzoo!henry@uunet.UU.NET>
Sat, 10 Sep 88 00:25:26 EDT

>How many computer professionals have noticed the continual technical
>improvement of video games in the past couple of years, and the
>concomitant decline of their social and moral content? ...

As has been pointed out in the past, this is silly. The social and moral content of chess or Monopoly is also deplorable, looked at from the same viewpoint. (Chess is a wargame; the objective of Monopoly is to drive your friends and relatives into bankruptcy.) Video games only make it a bit more obvious. Wargames, in particular, long predate video games. Is it less moral to strafe the bad guys in a video game than to condemn thousands of hypothetical troops to death by moving a counter on a board? Which is more depersonalizing?

Henry Spencer at U of Toronto Zoology

"Viruses Don't Exist" and the Marconi Mysteries...

Mark Moore <MARKO@s55.prime.com>
Wed, 07 Sep 88 17:30:40 EDT

I received one of those info-card packs (I forget from whom) as a result of having my name and address sold by Dr. Dobb's. I filled out a few of the cards and received a catalog from Public Brand Software, which is a shareware/ freeware clearing house based in Indianapolis, IN.

Here are a few quotes on from the third page of their catalog entitled 'Topic: VIRUSES'

> 'It seems like a couple of national magazines first thought up the concept of MS-DOS viruses. Unfortunately, a lot of people read these magazines and believe everything that they read. But let's get a couple of definitions clear first.
>
> virus, n. 1. a purposely destructive computer program that can propagate itself by modifying other computer programs (such as COMMAND.COM) to make them destructive. 2. a destructive myth perpetrated to sell a product and/or fill editorial space.'

The article goes on to claim that viruses are myths akin to friend-of-a-friend stories; popular magazines are perpetuating the myths to have something sensational to print; engineers are doing the same in order to sell vaccines. They claim that they've searched high and low and can find no such thing as a virus. 'Simply put, there is no such thing as a virus. There never has been. Period.'

Sounds like a dangerous attitude to me.

On a different note... For those interested in a book which follows a plot with a striking similarity to the Marconi incidents, try _The Chain of Chance_ by Stanislaw Lem.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 50

Monday 12 September 1988

Contents

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

"Computer glitch costs AA $50M ..."

<calvert@cs.utexas.edu>
Mon, 12 Sep 88 10:36:29 CDT

>From the Austin American-Statesman, Sun., 11 Sept. without permission:

Computer glitch costs American $50 million in lost ticket sales
by Martin Zimmerman, Dallas Morning News

FORT WORTH- American Airlines, Inc. lost as much as $50 million in potential revenue this year when its computerized reservations system mistakenly restricted the sale of discount tickets, driving price-conscious travelers to

American's competitors, the airline's chairman told industry analysts this week.

According to analysts who attended the metting in New York with Robert Crandell, American's chairman, president and CEO, the revenue loss was due to a foul-up in the airline's yield-management system. "(Crandell) said that early in the second quarter they had implemented a new software program, which appears to have backfired," said one investment company analyst, who asked not to be named. "It did not do what it was intended to do."

Yield management involves the use of sophisticated computer programs to determine how many seats on an airplane should be sold at various prices, squeezing the greatest possible revenue out of each ticket sold. On flights where there is heavy demand for seats, for instance, the program will instruct that fewer tickts should be sold at discount prices. On less-popular flights, more tickets will be sold at discount fares to fill what otherwise would be empty seats.

American is considered an industry leader in yield management. But when the airline modified its system this year, the new program contained a serious flaw.

According to the analysts, Crandall said the modified program prematurely stopped the sale of discount tickets for American flights, even though more seats would normally have been offered at lower fares. Travelers searching for a cheap fare -- told that none were available on American -- presumably then went to another airline to buy a ticket.

Lowell Duncan, American's vice president-corporate communications, said the problem went on for 30 to 60 days before it was discovered and corrected. It came to light when wide discrepancies cropped up in the number of discount tickets sold during the second quarter of 1988 compared to previous quarters....

News of the foul-up apparently didn't cause much of a stir among the analysts, who study airlines' financial performance and then make recommendations on whether investors should buy their stock.... "Had American had a poor quarter, this glitch might have been more of a problem," said Timothy Pettee, an airline analyst... As it was, American's yields -- the amount of money collected per passenger -- increased 13 percent in the second quarter, Pettee said. "They might've been up 15 to 17 percent without this glitch, which would've been phenomenal," he said.

This seems relevant to the recent discussions on quantitative risk assessment.

The $50 million figure must be regarded with suspicion in the absence of further information. (Does anybody besides me have a problem with phrases like "losses" in "potential" revenue?) Such numbers are meaningful only in context,yet it seems to be unavoidable in our society that, once created, they take on a life of their own and appear in isolation. In my experience the problem is not limited to the media. (Hence I am generally skeptical about quantitative methods in system design and certification.)

Ken Calvert

Risks of Motel Computers

Brint Cooper <abc@BRL.MIL>

Mon, 12 Sep 88 9:46:21 EDT

The following illustrates just how ignorant the "general public" remains of issues that the Risks community almost take for granted.

Last month, with a friend my wife and I were touring Southern Maryland. We stopped unannounced at a new Holiday Inn and booked two rooms in my name. With both rooms' keys in hand, we proceeded to our friend's room; I opened the door to check out her room and found that the room was not vacant. While no one was actually in the room, briefcases, books, and clothes made it evident that someone else was already booked therein.

Angrily, I returned to the desk, explaining to the very young night staff there the real risk of such an error: that the room might be occupied by a handgun-toting paranoid who would shoot first and ask questions later. The young woman offered that "the computer must have made a mistake." I slightly mis-represented myself as a "computer scientist" and told her that this was no excuse and repeated all the arguments that are more than familiar to readers of "Risks Digest." We were assigned another room.

At checkout the next morning, I reported the mistake to the morning staff, so that "management" would become aware. After the expected profuse apologies, the desk manager said, "The computer shouldn't have allowed that. The night clerk must have made a mistake."

What could I say?

Brint Cooper

IFF and the Vincennes

"Geoff. Lane. Tel UK-061 275 6051" <ZZASSGL@CMS.UMRCC.AC.UK>
Mon, 12 Sep 88 09:32:13 BST

Once upon a time I worked on the IFF software of the Nimrod project. (Nimrod was a British Airborne Early Warning system which got cancelled - to be replaced by AWACS). As part of the design process we were given a few lectures on the purposes and uses of IFF in general. During these we found out that

a) NO combat fighter plane will ever go into combat with its IFF system operating - for obvious reasons!

b) If you are in a combat zone and a planes' IFF claims it to be a civilian assume that it is a counterfeit signal.

These policies were not, to my knowledge built into the software. They were left for the pilot to act upon. This was about 10 years ago now. I doubt if the general policy of the UK air defence people has changed. It would appear that the Captain of the Vincennes worked to a similar set of assumptions.

BTW, The Nimrod project was done by GEC-Marconi Space and Defence

Systems. This is a part of the same company that is currently being so unlucky with suicides and strange accidental deaths.

Geoff. Lane., University of Manchester Regional Computer Centre

---

"Single keystroke"

"Philip E. Agre" <AGRE@AI.AI.MIT.EDU>
Mon, 12 Sep 88 03:50:09 EDT

PGN attaches the following comment onto a message about the Soviet's loss of a Phobos spacecraft.

[Several people reported on radio items that attributed the problem to a console operator's single keystroke in error, which it was speculated might have triggered the Mars probe's self-destruct signal. After the command was sent, contact with the probe was lost completely. PGN]

I have no reliable information about this particular case, but I am struck by the high proportion of operator mistakes which get reported as `single keystroke' errors. I strongly suspect that single-keystroke errors are largely an urban myth (you know, poodles in microwaves and the like). I'm sure that in this world of crummy user interfaces you can often do plenty of damage with a single keystroke, but the image of a single mistaken keystroke leading to disaster has got to be a very tempting trope for journalists and cartoonists and rumor-passers whether it's accurate or not. Besides, it'll always have a certain tenuous relation to the truth: the single keystroke that does the damage is the final Return you hit after your two hundred keystrokes of wrongheadedness.

`Credit doctors'

Donn Seeley <donn@cs.utah.edu>
Mon, 12 Sep 88 00:46:26 MDT

Clean Credit for Sale: A growing illegal racket
by Larry Reibstein with Lisa Drew, Newsweek 9/12/88 p. 49

Houston schoolteacher Darlene Alexander thought she had a clean credit record. Then in June she applied for a $75,000 mortgage, and the lender told her she had too much debt to qualify. Her records showed accounts for American Express, MasterCard and Visa. The biggest balance was a $22,800 loan for a 1988 Chevrolet Camaro. All this baffled Alexander. None of the accounts were hers; she drives a paid-up 1983 Datsun. Alexander was a victim of 'credit doctors,' people who use computers to steal good credit histories and then sell that information to people with bad credit. Using Darlene Alexander's name and history, an impostor opened charge accounts and got loans with almost no risk. The real Alexander, who was also turned down for a vacation loan, is angry. 'You try for years to get good credit,' she says, 'and then someone else just takes it away from you.'

Credit doctors -- thieves, really -- are starting to surface in a big way. In Houston, where the depressed economy has created plenty of willing customers, about 30 people have been arrested, and 20 convicted, for credit-doctoring schemes in the last year. Among them were 'patients' -- consumers -- who paid up to $2,000 for stolen or fake credit identities. Houston police have identified $7 million to $10 million in merchandise and homes bought with the help of fraudulent accounts. Similar cases have cropped up in Chicago and Los Angeles. In an era when everyone seems intent on building up their credit one way or another, Secret Service agent Neal Findley says, 'An industry has risen up based on getting into other people's credit files.'

The thieves work by tapping credit-bureau computers that contain histories on millions of consumers. It's surprisingly easy. Credit doctors usually buy the computer-access code from a contact who works in a legitimate business, such as a mortgage company. Using a personal computer, the credit doctor searches for someone who has his client's name -- and good credit. He then copies that person's credit history -- including the all-important social security number [[argh! -- Donn]] -- and furnishes the information to the client, who uses it when applying for credit. Houston police say some consumers have been offered a choice of credit histories at a range of prices, depending on the 'quality' of the stolen credit. ...

Authorities believe many credit-doctoring scams remain undetected. People whose histories have been stolen may never know it -- until a lot of debt is entered in their names. Merchants often look the other way as long as the impostor is keeping up with payments, says Houston police lieutenant J. F. Rabago. Many credit bureaus say that no safeguards can completely block unauthorized access to their computers. For now, a consumer can only hope that someone with the same name isn't in the market for a new credit history.

[[Are credit bureaus' security measures really this lax? It's not hard to believe, just appalling. -- Donn]]

Scientific Safety

<WHMurray@DOCKMASTER.ARPA>
Sun, 11 Sep 88 13:22 EDT

Since I only speak American, I often have a difficult time understanding things originating across the pond. For esmaple, Bev Littlewood writes:

>The system is certificated in Europe, the thing is carrying passengers,
>yet, I believe, it cannot be asserted in any scientifcally meaningful
>way that it has an "acceptable level of safety".

It is not clear to me whether "scientifically meaningful" modifies "can be asserted" or "acceptable level of safety." It seems to me that a great part of this discussion has turned on whether "acceptable level of safety" can ever be a scientific term.

It sounds to me as though it is being asserted that in the UK it is a scientific and, even legal, term. I would assert that in the US it is neither.

It is at best political, and at worst journalistic. The toleration of a risk in the US is inversely proportional to its novelty or its mystery.

We do not tolerate the risk of the medicinal use of marijuana or heroin in terminally ill patients. On the other hand we tolerate 300,000 premature, painful and slow deaths a year from the use of tobacco. We tolerate 1500 to 10,000 measureable deaths a year from the burning of fossil fuels. Much lower risks of alternatives cannot be tolerated because of the absence of political courage. We kill 40,000 people a year on our highways, and maim for life another 2-400,000, while programs in other countries suggest to us that least half of those are avoidable.

Novel technology, such as fly-by-wire, would not be tolerated here unless it could be "proved" to be safer than the technology in use. (The opposition to the A320 in the US revolves around the fact that it contributes to an unfavorable balance of trade and has a two man cocpit. The opposition has missed a good bet. The risk of new foods and drugs here are measured absolutely, in terms of their risk in small animals; not against the risk of the alternatives. Better the devil we know.

One can say little "scientific" about safety and risk in such a society.

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

Bev Littlewood's message in RISKS-7.48

Peter G. Neumann <Neumann@KL.SRI.COM>
Sun, 11 Sep 88 20:28:20 PDT

Somewhere between Bev's transmission to Brian Randell and Brian's retransmission to me, Bev's lines longer than 80 characters got truncated. Sorry. [Probably at the border? Customs? Round up the usual characters?]
[By the way, I sometimes get messages from within the U.S.A. whose text has NO line breaks -- just rampant character strings. The UK/USA 80-character filter would truncate the entire message except for the first 80 characters!]

Calculations with Wrapped Numbers

Mark Brader <msb@sq.sq.com>
Fri, 9 Sep 88 17:41:38 EDT

> > The problem occurs when the previous value is -175 or so and the new
> > value is +175. What is the average?

> A good way to estimate an average angle, A, from a set of angle measurements
> a[i] 0<=i<N, is ....

The reason that this problem is a problem is that in modular arithmetic -- which is what we're talking about here -- there *is* no such thing as an

"average", at least not in the usual sense of "arithmetic mean".

It would probably help, then, if people would be careful to define their terminology.

The "average" algorithm that the second-cited poster gave arises as follows. Represent the modular arithmetic as a circle (the original physical representation in this case); take each angle value as a vector, all of equal length; sum (or average, doesn't matter) all the vectors; and translate the direction (if any) of the resultant back into a numeric angle value. I guess this is indeed correct for problems where it makes sense to speak of an average angle, but it may be useless for other problems involving "averaged" modular numbers.

Mark Brader, SoftQuad Inc., Toronto

Calculations with wrapped numbers (Re: RISKS-7.44)

<Bennet.Yee@PLAY.MACH.CS.CMU.EDU>
Tue, 06 Sep 88 10:03:56 EDT

karsh@sgi.com suggests using trig

$$a = \arctan\left(\frac{\sum_{i=1}^{N} \sin(a[i])}{\sum_{i=1}^{N} \cos(a[i])}\right)$$

to average angles. This forces us to perform consistency checks to figure out which quadrant the angle is really in. Otherwise, we may get incorrect results (risk of using posted algorithms?). Perhaps a simpler algorithm would be to view the angle measurements as [unit] vectors and average the vectors together. Not only is this conceptually simple, it also allows incorporation of measurement reliability by scaling the vectors.

[Similar comment from Mark Mandel...]

Re: Calculations with wrapped numbers

<wolit@research.att.com>
Tue, 6 Sep 88 16:28 EDT

You take the average of the sines of the angles and the average of the cosines of the angles, divide, and take the arctangent of the result.

Jan Wolitzky, AT&T Bell Labs, Murray Hill, NJ; 201 582-2998; mhuxd!wolit

---

RE: Calculations with wrapped numbers and risks of roundoff

Magister ludorum <goun%evetpu.DEC@decwrl.dec.com>

6 Sep 88 15:24

<> Imagine trying to compute the average position of the second hand on a
<> clock. You sample the position once a second for sixty seconds. Ok, now
<> what is the average?

I made a deliberately naive attempt to determine the average position of a second hand, using the above formula and a spreadsheet program that shall remain nameless. I assumed N = 60, 0 <= a[i] <= 354. The spreadsheet dutifully reported that sum_i_from_1_to_N sin(a[i]) = -7.173E-10, sum_i_from_1_to_N cos(a[i]) = .000000014, and a = -3.0000006.

This example is obviously contrived to "make the computer look bad." But it's not hard to imagine a scenario in which such a completely bogus answer might seem plausible to an unsophisticated consumer of information, especially if he or she was not shown the intermediate results of the calculation.

Roger Goun

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 51

Tuesday 13 September 1988

Contents

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

Single Character Errors

"Geoff. Lane. Tel UK-061 275 6051" <ZZASSGL@CMS.UMRCC.AC.UK>
Tue, 13 Sep 88 11:07:15 BST

It has been suggested in a previous RISKS that single keystroke errors may just be an Urban Myth. Unfortunately not - in the GEORGE 3 operating system (which used to run on ICL 1900 series computers) the command to edit a file was "ed" and the command to erase a file was "er". The letters "d" and "r" are conveniently next to each other on the keyboard.

Apart from this one aberration the George 3 system was a great improvement

on all its successors!

Geoff. Lane., University of Manchester Regional Computer Centre

---

Soviet Mars Probe

Peter G. Neumann <Neumann@KL.SRI.COM>
Tue, 13 Sep 88 15:20:18 PDT

For the "single-character" doubters:

The Soviet Mars probe was mistakenly ordered to "commit suicide" when ground control beamed up a 20 to 30 page message in which a single character was inadvertently omitted. The change in progam was required because the Phobos 1 control had been transferred from a command center in the Crimea to a new facility near Moscow. "The [changes] would not have been required if the controller had been working the computer in Crimea." The commands caused the spacecraft's solar panels to point the wrong way, which would prevent the batteries from staying charged, ultimately causing the spacecraft to run out of power.

[From the SF Chronicle, 10 Sept 88, item (page A11), thanks to Jack Goldberg.]

Stanford Collider Shut Down

Peter G. Neumann <Neumann@KL.SRI.COM>
Tue, 13 Sep 88 15:35:20 PDT

Stanford University's $115 million linear collider has been shut down after several months' efforts failed to get it running properly. Although there seems to be nothing basically wrong with the system, it is "simply so complicated that, despite the best efforts of more than 100 people, they have not been able to keep all its complex parts working together long enough to get results." Since spring they have "fought a succession of glitches and breakdowns in the machine's myriad magnets, computer controls, and focusing devices." [Source: San Francisco Chronicle, 13 September 1988, p. A2]

Destructive remote controls

<williams@CSS.NRL.NAVY.MIL>
Tue, 13 Sep 88 13:26:56 EDT

Recently, I was in a hotel room in the Washington, DC area. The TV in the room had a remote control that was not, as is often done, anchored to the bedside table, but did have this theft-deterant notice on it:

> "This remote control will only work on Beeblebrox Hotel TVs.
> REMOTE WILL DAMAGE your home TV sets."

The first sentence I believe, the second I absolutely do not. I can not imagine what form the damage might take, unless the IR coming from the remote is so bright that it would burn out the sensor in an "ordinary" TV or VCR. So, is this notice a lie, to decrease the likelyhood of theft? That's all I could figure, but it sure reduced my opinion of Beeblebrox Hotel for putting such a silly notice on the thing.

Why am I posting this to RISKS? Well, suppose it's true! What damage could I do with this "infrared laser"? Will it hurt my eyes? If I had an HP-28 calculator, or similar device, which uses an optical connection for the printer, could I accidentally damage that? Had I been an actual paying guest I would have harassed them about it, but I was just visiting and it was on a weekend, so I doubted I'd find out anything useful.

Technical information: The remote (and TV) were made by General Electric, it was powered by two AAA cells, and seemed to be a typical IR controller, but with minimal functions. "Beeblebrox" is not the true name of the hotel ;-).

Jim Williams

Re: computer follies

Mark Brader <msb@sq.sq.com>
Mon, 12 Sep 88 14:55:19 EDT

Path: sq!utfyzx!utgpu!utzoo!attcan!uunet!mcvax!unido!sbsvax!greim
From: greim@sbsvax.UUCP (Michael Greim)
Date: 7 Sep 88 09:29:05 GMT
Organization: Universitaet des Saarlandes, Saarbruecken, West Germany

Here are some computer follies published some time ago.

>From Jack Campin (jack@cs.glasgow.ac.uk) on Nov 27 1987

<I have had the doubtful privilege of looking after an ICL 3930 over the last
<
<To test out new user interfaces, Xerox would videotape novice users
<
<Upon review of the tape, the researchers discovered that the person was
<'i').

>From Clif Flynt (clif@.chinet.UUCP) 15 Dec 1987 :
<In article <1943@ncr-sd.SanDiego.NCR.COM> matt@ncr-sd.SanDiego.NCR.COM (Matt Costello) writes:
<>The real problems in interface design generally occur because of
<>unstated assumptions. We had a hilarious incident occur here
<>recently...
<>
<> Imagine our suprise when a worried secretary called
<>to say that she had been able to fit only 5 of the disks into the
<>disk drive.
<>
<

< A similar incident happened to a friend, diagnosing a floppy disk read
< "Have you cleaned the disk?" He inquired, thinking that the heads might
< "I'll try it and call you back", said the person at the other end, and
<
<
< There is also the tale of the DP manager who wanted to make sure that
<
< Another friend of mine tells the tale of a system where people
< It finally turned out that two key-caps on the keyboard had been swapped.
<When people sat, they put their fingers on the 'home row' and typed,

---

IFF and the Vincennes

<brantly.henr@Xerox.COM>
13 Sep 88 10:11 EDT

In response to the Geoff. Lane msg of Mon, 12 Sep 88 09:32:13 BST; "IFF and the Vincennes" in which he stated:

> "a) NO combat fighter plane will ever go into combat with its IFF system operating - for obvious reasons!"

I must disagree.

My understanding is that there are 3 catagories in which a "bogy" will be placed, depending on the IFF, or absence of IFF:

1> Friend
2> Foe
3> Unknown

IF a ship finds itself in a COMBAT situation and detects an aircraft which is approaching and which is not of catagory 1, then the ship will more than likely fire.

The only way that an aircraft can be determined to be a FRIEND is either by having correct IFF or by visual comfirmation. An aircraft with NO IFF, will be of catagory 3 (Unknown), but if considered approaching in a threatening manner (ship's determination not the pilot) will quickly be changed by default to catagory 2 (Foe) and will be fired upon.

You might ask what is to prevent an "enemy" aircraft from being classified as a FRIEND? Elaborate measures ARE in place to prevent this from happening, HOPEFULLY they are adequate. It is because it is easier to "turn the IFF off" (becoming catagory 3 rather than 2) than break the codes necessary to become catagory 1, that makes the Unknown aircraft so likely to be fired upon in a combat situation.

So my argument is that if a friendly aircraft is operating in an area where there are also friendly forces, it had best keep its IFF "ON" or "risk" that it's own forces may shoot it down.

In the "heat of battle" each individual ship must make fast decisions based on

the information it has available to it at that time (IFF). Those decisions ultimately determine the fate of the ship/crew/mission.

Case in point:

Vietnam, 1972

I was the operator of MR3, Missile Radar #3 (AN/SPG 51-C) on the USS Towers (DDG-9) off the coast of Haiphong Harbor, North Vietnam, approx. 3AM. We were in the process of shelling various railway yards and also taking fire from 175mm shore batteries when a low-flying, high-speed aircraft was detected heading towards our ship at approx. 12 miles distance, with no IFF.

The plane was immediately assumed hostile, both MR2 & MR3 were assigned the target. MR3 "locked on" first. 2 "birds" (standard - missiles) were loaded on the launcher, and the launcher was assigned to MR3. At that time the target was within only 1 - 2 seconds from being fired upon.

It was a US F-4 phantom fighter. He detected our "intent to launch" and QUICKLY turned on his IFF. The launcher was unloaded (you don't want to leave live missiles on the rail when you're taking hostile fire from shore batteries!) and MR3 was then unassigned.

IFF was the only thing that prevented us from firing at, and more than likely shooting down, one of our own aircraft.

I guess my point is that having your IFF "turned off" doesn't really buy you anything, at least not in a "combat" situation. Perhaps in a "sneak attack" during peace time, when you would more than likely be given the benefit of the doubt, but not once a conflict has started. Anti-ship weapons (and their launch platforms) have become too sophisticated, their warheads too powerful, for a Captain to risk his ship & crew on being wrong.

Dennis

Re: Disinterest in disaster not based on probability estimates

Amos Shapir <amos@taux02.UUCP>
12 Sep 88 22:44:06 GMT

Clifford Johnson (RISKS-7.51) complained about the public's disinterest in disasters vs. their interest in the lottery, even though the former's odds of occurring are much greater.

I'm afraid the public's view is understandable even from the statistical point of view: the odds of winning the lottery are slim, but it does happen to somebody somewhere every week; a nuclear disaster is rare, and so far each of the few that did happen caused less casualties than a major airliner crash, and all the victims were concentrated in a small area. Anyone outside such an area is safe. It's this 'lumping' of consequences that distorts the calculation of statistical odds.

Amos Shapir, National Semiconductor (Israel) P.O.B. 3007, Herzlia 46104, Israel

Tel. +972 52 522261 TWX: 33691, fax: +972-52-558322

``MS-DOS "virus" programs do not exist.'' (Re: RISKS-7.49)

David Dyer-Bennet <ddb%ns%bungia@umn-cs.cs.umn.edu>
12 Sep 88 22:35:54 GMT

In RISKS-7.49, Mark Moore writes about a public-domain software catalog containing an article claiming that MS-DOS "virus" programs do not exist. I view this with a certain glee, because for several years I've been attempting to follow up each story about viruses I hear; so far, the story has either faded into the distance, or I have been told that they have the virus isolated, but won't show it to me. While I accept that people running academic computer centers, in particular, have some justification for taking a paranoid attitude (though I wasn't approaching them from within as a student), I've been telling people for some time that by covering up viruses the way they do, they are going to lead people to believe it's all a myth, which in the long run is bad. So let me just say, "I told you so." to those who've been concealing the evidence.

-- David Dyer-Bennet, Terrabit Software

...!{rutgers!dayton | amdahl!ems | uunet!rosevax}!umn-cs!ns!ddb
ddb@Lynx.MN.Org, ...{amdahl,hpda}!bungia!viper!ddb
Fidonet 1:282/341.0, (612) 721-8967 hst/2400/1200/300

Hiding payoff slot (Re: RISKS-7.42)

<ficc!peter@uunet.UU.NET>
Tue, 13 Sep 88 11:47:06 EDT

> Modified games must have some sort of mechanism (either mechanical or human)
> to pay off a win. ... jim frost

The gambling mechanism already exists in most vending mchines these days, and could be easily justified as part of a videogame. This mechanism is a change slot. If the game gives change under computer control, it can easily be modified to handle the payoff as well.

Also, many video-games these days have a 'challenge mode', where you can send in for a tee-shirt if you beat a particularly hard level. Perhaps this could be considered gambling?

Peter da Silva, Ferranti International Controls Corporation

Citation for "car engines become target for hackers"

<karl%ficc@uunet.UU.NET>
Wed Sep 7 15:24:11 1988

Readers seeking more information about car engine computer hacking are directed to the article "Electronics puts its foot on the gas" in the May 1988 issue of "IEEE Spectrum." The article profiles a couple of companies working in this area. While one company had reverse-engineered source code and was using in-circuit emulators to debug their changes, another was merely substituting values into an array they'd located. The tone of the article was not as negative as that quoted from "The Australian" by George Michaelson in RISKS DIGEST 7.39. A company specializing in BMWs had done a lot of business directly with dealers desperate to fix acceleration problems in some customers' cars.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 52

Wednesday 14 September 1988

Contents

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

Tom Wicker column on computers, Vincennes and SDI

Gary Chapman <chapman@csli.Stanford.EDU>
Tue, 13 Sep 88 15:39:05 PDT

Tom Wicker, the famous columnist for the New York Times, has a column in the Times today about computers, the Vincennes incident, and the SDI. Wicker has picked up on a story John Markoff has been working on for some time, on whether complex computer networks exhibit chaotic behavior similar to the mathematical phenomenon of chaos found in nature. Wicker says that "these two events [the Vincennes and a problem with a TRW computer that John described in one of his articles] were unrelated except that they offer a common warning against too complete reliance upon computers and electronic systems as substitutes for or multipliers of mankind's innate abilities."

". . . Star Wars will be heavily dependent upon a vast network of sensors, computers and electronic weapons guidance systems girdling the globe and only nominally under human control.

"Given the likelihood of breakdown at any of thousands of points in a system so complex that no one has been able as yet even to design the software, it takes a leap of faith to believe that the SDI would increase national security against attack. More likely, aping the computers at your local bank or an airline ticket counter, the system would be 'down' when most needed."

Wicker then goes on to speculate on the dangers of an SDI computer system subject to chaotic behavior. Wicker quotes a professor of electrical engineering at MIT, William Schreiber, who notes that the Aegis system in the Gulf was at least responding to something that everyone on board had been trained to deal with and had probably actually seen, i.e., a commercial airliner radar signature. What will happen with SDI or ICBM crews who are presented with something no one has ever seen before?

"Not only may these high technology systems fail, or degenerate inexplicably into chaos, and be more prone to do so as they grow ever more complex; even when they function properly, the responses of the fallible human beings who may have to interpret their messages can be disastrous--and humans may be progressively less fit for a job so demanding.

"Thus, as we move inexorably into the world of high technology and control by computer, the undeniable benefits will not come cheaply. For mankind's enhanced capacities, the price may be that we diminish, rather than increase, what little dominance we have of our own destiny."

Computer error in vote tallying

Gary Chapman <chapman@csli.Stanford.EDU>
Tue, 13 Sep 88 15:24:27 PDT

The New York Times reported today that a computer entry error increased the vote count for the incumbent Lieutenant Governor of Delaware, S. B. Woo, and made it appear he had won the election when he may have lost. The correct number of votes in one district was 28, but the operator keyed in 2,828 by mistake. There will be a recount of the votes statewide.

Risks of Using Computers in Elections

Peter Neumann <neumann@csl.sri.com>
Tue, 13 Sep 1988 16:31:50 PDT

I noted in the July issue of the ACM Software Engineering Notes that there was a panel discussion at COMPASS '88 on the topic of computer systems for counting ballots. Two of the panelists have written reports that deserve mention here:

Lance J. Hoffman, ``Making Every Vote Count: Security and Reliability of Computerized Vote-Counting Systems'', Department of Electrical

Engineering and Computer Science, The George Washington University, Washington D.C. 20052, 2nd printing, March 1988.

Roy G. Saltman, ``Accuracy, Integrity, And Security In Computerized Vote-Tallying'', Institute for Computer Sciences and Technology, National Bureau of Standards, Gaithersburg MD 20899, NBS Special Publication, June 1988 (draft).

These two reports are absolutely essential reading for anyone interested in the problems arising in election software. There is also a paper by Erik Nilsson ("A Bucket of Worms") on this subject, in the proceedings of CPSR's DIACS 88.

Soviet Space Probe

<dcf@ALLSPICE.LCS.MIT.EDU>
Wed, 14 Sep 88 09:00:46 EDT

A friend of mine who does satellite work expressed surprise that the Soviets could lose a space probe so easily. Apparently, US craft have a "panic" mode that takes over if there is some problem (presumably in this case the batteries running low). The probe then realigns itself so that its solar panels face the sun, its antenna faces the Earth and it waits for new commands. This seems like the right idea, but I don't know much about how it works. For instance, are the panic commands in ROM so that they can never be overwritten?

Dave Feldmeier

Re: "Single keystroke"

Matthew P Wiener <weemba%garnet.Berkeley.EDU@violet.berkeley.edu>
Tue, 13 Sep 88 22:39:01 pdt

On Unix, even experienced users can do a lot of damage with "rm". I had never bothered writing a safe rm script since I did not remove files by mistake. Then one day I had the bad luck of typing "!r" to repeat some command or other from the history list, and to my horror saw the screen echo "rm -r *" I had run in some other directory, having taken time to clean things up.

Maybe the C shell could use a nohistclobber option? This remains the only time I have ever rm'ed or overwritten any files by mistake and it was a pure and simple gotcha! of the lowest kind.

Coincidentally, just the other day I listened to a naive user's horror at running "rm *" to remove the file "*" he had just incorrectly created from within mail. Luckily for him, a file low in alphabetic order did not have write permission, so the removal of everything stopped early.

ucbvax!garnet!weemba Matthew P Wiener/Brahms Gang/Berkeley CA 94720

London Underground problem

"Lindsay F. Marshall" <Lindsay_Marshall%newcastle.ac.uk@NSS.Cs.Ucl.AC.UK>
Wed, 14 Sep 88 13:46:43 WET DST

According to the news on the wireless this morning the London Undergound system was distributed by a power failure that had damaged "the computer". This system appears to control all the lifts, escalators and signals!!
Anyone know what really happened??
Lindsay

Re: Destructive Remote Controls

<Curtiss@DOCKMASTER.ARPA>
Tue, 13 Sep 88 20:54 EDT

Jim Williams writes of a remote control at a hotel which had the ominous warning on it:

> "This remote control will only work on Beeblebrox Hotel TVs.
> REMOTE WILL DAMAGE your home TV sets."

He then asks if this is indeed possible.

I believe that it is entirely possible. The control signals for the remote could be chosen in such a way that the "on" control would send a command stream that would be interpretted by a home TV set as "on" immediately followed by "off". Such cycling of the power will quickly damage the power control circuit and send spikes to the rest of the components. Most TVs require some form of delay between an "on" and an "off" (actually, they are the same code, the TV just changes state) but this could easily be accounted for.

For those doubters, I heard of a "crt saver" for the IBM a long time ago that actually destroyed the monitor. It would cut one of the locking frequencies (I believe that is how it worked) which would make the sceen appear blank, but would allow a charge to build on a capacitor. Eventually the capacitor failed and took the rest of the monitor with it.
William Curtiss

An ANI Compromise

<linnig@skvax1.csc.ti.com>
Tue, 13 Sep 88 17:37:47 CDT

> The `privacy' argument has two sides.... it is the right of an individual
> *not* to have their phone number displayed, but it is also the right of the
> individual *not* to answer anonymous calls. A problem to which the solution
> seems easy enough.... (now prove otherwise!)

[1] Suppose that all business phones had to "send" their phone numbers by law.

[2] Callers TO business phones have the right to withold their numbers using a prefix.

[3] Individual-to-individual calls would "send" their phone numbers unless a prefix was used.

[4] Individuals COULD have their phones set up so that any non-ANI calls would be rejected (with a recording saying why).

[5] If you dial a number with a prefix, you get a recording if the target of the call ALWAYS gets ANI (e.g. the police emergency line); the call will complete at the callers option.

I suspect most folks would opt for [4] on their home phones. This should cut down on the number of obscene calls. AIDs hot lines can be called with the prefix -- the caller knows their number is not being traced because they did not get a recording. Callers to businesses know their number is not being traced if they used a prefix.

Does that solve some of the problems?

Mike Linnig, Texas Instruments

RISKS Guidelines revisited [*** PLEASE READ THIS. ***]

Peter Neumann <neumann@csl.sri.com>
Tue, 13 Sep 1988 17:13:19 PDT

In the interest of keeping RISKS stimulating, and minimizing the mass of suboptimal submissions, this is a reassertion of and elaboration upon a few of the masthead guidelines, from mechanical to contextual.

CONCISE: Short contributions are strongly preferred, assuming they satisfy the other criteria. Long ones may wait indefinitely, unless they are very hot. I would rather not have to impose a default limit, but would like to urge consideration on your part. Think of all the times you have had to struggle with reading someone else's overly long messages that wandered illogically, and try not to write that way.

NONREPETITIOUS: Messages that go over the same ground as previous messages (including this one!) place a serious burden on all of us. I cannot remember every contribution, but try very hard to minimize repetition. Please try to check over previous issues before you fire off your comments. When you relate to back issues, do so explicitly. Messages that blindly incorporate an earlier message in its entirety (particularly when it is long) are very annoying. Yes, I tend to delete most of the repeated portions, but you might better do that yourselves. Interstitial annotations that comment almost paragraph by paragraph on the earlier messages are generally not very interesting anyway, so avoid those altogether. (By the way, I usually keep reconsidering not-yet-included but still-possibly-interesting messages for several days until they eventually fall off the end of my attention span. However, I do not usually send out rejection notices, and trust the network

servers to help you distinguish between that case and the case in which your mail was never received -- although that may not be a reliable process for some of the networks.)

COHERENT: Writing skills are difficult to master. But PLEASE take care in formulating your thoughts. It makes your contributions much more readable, and saves agonizing back-and-forths later. I hate playing English professor, but I cannot believe how bad some of the submitted writing is. (I do edit when it is flagrant.)

RELEVANCE: By now you know that I have a broad interpretation of "computers and related systems". But I still get lots of contributions that are clearly not relevant.

There are a few of you RISKS contributors whose messages have been reliably relevant, sound, concise, etc., and who always assume other readers are smart, honest people with good intentions. Many thanks to you. I hope that others will try harder to emulate you. As a reward for you, this relatively boring message is placed last in the issue (just in case you didn't get this far) -- in the ongoing struggle to make RISKS readable. (For some others, however, it probably should have been placed FIRST.)

Thanks to all RISKS folks for your support and help over the past three years. The feedback I get seems to indicate that it is worth the effort to continue.
Peter

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 53

Thursday 15 September 1988

Contents

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

Hurricane Gilbert

Matthew P Wiener <weemba@garnet.Berkeley.EDU>
Thu, 15 Sep 88 03:32:05 pdt

The following appeared in ucb.general:

From: netinfo@GARNET.BERKELEY.EDU (Postmaster & BITINFO)

Hurricane Gilbert may cause various national and international

network links to fail or to be closed down. The follow message pertains to BITNET links in the mid-US. Links to Mexico and South America may also be affected.

Date: Wed, 14 Sep 88 13:15:17 CDT
From: "Richard A. Schafer" <SCHAFER%RICE.bitnet@jade.berkeley.edu>

Hurricane Gilbert is approaching the Texas coast. If it appears to be heading into the Houston area, or close enough to it to cause serious problems, Rice will close down for an indeterminate time period, until the danger of the storm is past. If the hurricane does in fact come through the Houston area, storm damage may cause power outages; the last hurricane in 1983 caused power outages of various lengths from a few minutes to several days. We will try to keep you informed.

The storm should hit the coastline Friday or Saturday.

Richard

Phobos I details

Dave Fiske <davef@brspyr1.brs.com>
Tue, 13 Sep 88 13:56:06 edt

from The Schenectady Gazette, Sept. 10, 1988.

SOVIET MISTAKE LED TO 'SUICIDE' FOR MARS PROBE

"Houston (UPI) - One of two ambitious Soviet probes hurtling toward Mars was mistakenly ordered to 'commit suicide' when ground control beamed up a long series of radio commands that included a single incorrect letter, a top Soviet space official says.

"The Houston Chronicle reported yesterday in a copyright dispatch from Moscow that Roald [sic] Sagdeev of the Soviet Institute of Space Research in Moscow said it would be 'a miracle' if the Phobos 1 probe could be saved.

* * *

"Sagdeev told the Chronicle the trouble began when control of the Phobos 1 spacecraft was transferred from a command center in the Crimea to a new facility near Moscow.

"'The controllers did not estimate how difficult it would be to work in a new environment [near Moscow]', he said.

"Sagdeev said the flight controllers had to prepare a long message to the computer of 20 to 30 pages, and in that message, a controller left out one letter.

"'The [changes] would not have been required if the controller had been working the computer in Crimea', he said. When the flight controller

sent the incorrect message to the computer, 'by an unbelievable small chance' there was a failure in the computer that allowed the error to go undetected.

"In the end, he said, the absence of one letter from the computer programming and the absence of a computer backup program, resulted in the transmission of 'a comment [sic] to commit suicide' to Phobos 1."

Phobos I details

Jack Goldberg <goldberg@csl.sri.com>
Thu, 15 Sep 88 09:47:24 -0700

Key phrases in the Phobos report:

1. ...by an unbelievably small chance, there was a failure in the computer that allowed the error to go undetected.

2. ..and the absence of a computer backup program..

In (1), the issue seems to be error detection, such as is given by a check on character type (probably not the case because of reference to a missing character) or a longitudinal check on a character string or substring (parity, sum, count, etc.) Such checks may be performed in hardware or in software. In (2) the problem is characterized as the absence of a backup program, which is not, strictly speaking, an error detection mechanism, but rather a remedy that may invoked by detection of an error (an alternate remedy is to notify an operator). Error detection is arcane computer stuff, while "backup program" is almost daily english. My guess is that the problem was indeed a failure in error detection, and that the reporter mischaracterized it as a failure in backup. In either case, it seems that the failure was caused by a combination of human and computer system failures.

By the way, failure in error detection (and recovery, too), is a major type of system error (e.g., reports by Siewiorek, CMU, and Iyer, U. Ill.) The standard explanation is that since errors are rare events, error detection mechanisms are less frequently exercised and hence are more poorly debugged than the rest of the system.

Jack

Computers and Elections

Lance J. Hoffman <LANCE@GWUVM.BITNET>
Thu, 15 Sep 1988 14:51 EDT

RISKS readers in the DC area may be interested in knowing that CPSR/DC chapter is sponsoring a panel discussion on "Accuracy in Computer-Tabulated Elections" Tues Oct 4, 7:15-9:30 pm at Room B120, Academic Center, 22 and I St. NW, George Washington Univ., Washington, DC (Foggy Bottom metro). Participants are Roy Saltman, NBS; me; Carol Garner, Director of the Election Center (a nonprofit organization for election officials; the closest thing they have to the ACM,

and moving slowly in that direction); and Eva Waskell, an activist whose name stirs fear into the hearts of election officials across the country. If you're in town, stop in; it should be a good show.

Lance

The First "Virus" on Japanese PC

Yoshio Oyanagi <oyanagi@is.tsukuba.junet>
Wed, 14 Sep 88 13:35:04+0900

PC-VAN, the biggest Japanese personal computer network operated by NEC, was found to be contaminated by a kind of virus, several newspapers reported today (September 14). This is, as far as I know, the first virus reported on a Japanese PC. The viruses so far reported in Japan were all on American PC or WS. PC-VAN is a telephone based network between NEC PC9800 personal computers, the best sold PC (> one million) in Japan.

This virus does not destroy programs or data unlike those in US, but it automatically posts the user's password on the BBS in crypto- graphic form. The offender will later read the BBS and obtain the password.

Several members of PC-VAN claim that they are charged for the access to PC-VAN which they do not know. This virus seems not to be contagious by its own power. The PC9800's OS was contaminated when the user carelessly run a anonymously distributed program on the PC.

Another one-key mishap

Larry Nathanson <lan%bucsb@purdue.edu>
15 Sep 88 20:47:52 GMT

On the 'one key bringing the house down' front: On the machine here, (and I suppose, on many multi-user machines under UNIX) if a user wishes to kill the first job, waiting in his/her job queue, s/he types:

kill -9 %1

I've heard that upon occaision the system operator will type:

kill -9 1

Since the operator can kill ANY job, it works. Job number 1 is a critical process that maintains the multi-user status of the machine. Once the above command is entered, the operator is the only user on the machine. (Though he may not realize it for a while!)

I'd hate to think what the analogue to this would be in the star wars system!

-Larry Nathanson

[(By the way) RISKS is performing a very important service: It is written by, and read by those who really should be informed by it- the computer professionals of today and tomorrow. If they (we) do not appreciate and understand the risks of computers, then noone will.]

Re: "Single keystroke"

<wrc%vienna@CS.RIT.EDU>
Thu, 15 Sep 88 08:47:07 EDT

Matthew P Wiener writes:
>On Unix, even experienced users can do a lot of damage with "rm"...

A similar situation occurred here a few months ago. A student went to his instructor for help in removing a file named "-f" from his account. The instructor first attempted "rm -f", which didn't complain but also didn't remove the file. After a few similar attempts, the instructor fell back on the tried-and-true method of "rm -i *". Some time passed during which no messages appeared on the terminal; as the instructor began to grow uneasy, the next shell prompt appeared. An "ls" showed one file in the directory, named "-f". At this point, the student (who had been watching the proceedings over the instructor's shoulder) commented, "If you weren't my teacher, I'd think you just deleted all my files."

Fortunately, the student hadn't done any work on the files that day, so all were recovered from the daily backup tapes. The problem in this situation was the interpretation by "rm" of the first file name, "-f", as an argument. The result was that the "-i" option actually given by the instructor was overridden by the name of the first file to be removed.

The blame for this event could be put in several different places:
UN*X command syntax (unlike VMS) doesn't sufficiently distinguish between runtime options and other arguments (e.g., filenames); the UN*X filesystem allows filenames which may look like valid options to commands; the "rm" command doesn't recognize potential incompatibilities between its options (i.e., "rm" shouldn't accept both the "-i" ("ask me before you delete anything") and "-f" ("don't complain, just remove these files") options in the same command line). It is hard to fault the instructor for not knowing that "rm" would override "-i" in this case, when (in his mind) he wasn't even specifying "-f".

Warren R. Carithers, Rochester Institute of Technology, Rochester NY 14623
rochester!ritcv!wrc wrc@cs.rit.edu wrc%rit@csnet-relay

Re: "Single keystroke" (RISKS-7.52, Matthew P Wiener))

Paul Dubuc <pmd@cbnews.ATT.COM>
15 Sep 88 12:48:10 GMT

Does C Shell have a way to display the command before executing it? In the Korn Shell you can type [ESC]/<pattern> to display the last command in your

history that matches <pattern> ([ESC]/r in Matt's example). If it's the command you want, you just need to hit [RETURN] to execute it. If not, you can type another `/` to keep serching or just edit the command and execute it. I have gotten into the habit of not using the blind repeat feature in the shell unless I'm certain that what will be executed is what I want.

Paul Dubuc, AT&T Bell Laboratories, Columbus

More computer follies -- how not to design a console

Seth Gordon <sethg@ATHENA.MIT.EDU>
Thu, 15 Sep 88 13:10:50 EDT

<To test out new user interfaces, Xerox would videotape novice users

---

GNU Emacs & Security (A.Gaynor via Eliot Lear)

the terminal of Geoff Goodfellow <Geoff@KL.sri.com>
Thu, 15 Sep 88 08:32:45 PDT

Return-Path: <lear@NET.BIO.NET>
Date: Wed, 14 Sep 1988 11:48:10 PDT
From: Eliot Lear <lear@NET.BIO.NET>
To: hackers_guild@ucbvax.Berkeley.EDU
Usmail: 700 East El Camino Real, Mtn View, California 94040
Phone: (415) 962-7323
Subject: [gaynor@aramis.rutgers.edu (Silver) : GNU Emacs & Security]

[The following was discovered by one of the Rutgers systems programmers. It is similar to the old "vi:" bug in that visiting a file may cause execution of an arbitrary set of commands including shell escapes... I am told that this has not been brought up on hg before.-eliot]

From: gaynor@aramis.rutgers.edu (Silver)
Subject: GNU Emacs & Security

This message is being sent to everyone in group slide. I've wandered across an application of a feature of GNU Emacs that may allow sliders to fall victim to trojan horses arbitrarily stuck in files. The feature in question is the `file variables' section of a file. Upon reading the file, portions of text may be evaluated, with perhaps profound results. For example, using this feature I was able to create a file that copied /bin/sh to my home directory, and chmod it to run setuid root. It wasn't hard at all. With a little effort, I'm sure I could have made its effects totally transparant.

So, protect yourself by inserting the following at the root level of your .emacs:

```
;; Protect thine arse from the Trojan file-variables section.
(setq inhibit-local-variables t)
```

The pertinent portion of this variable's documentation reads, "Non-nil means

query before obeying a file's local-variables list.". So, from now on, it's going to ask you if you want to process the variables if they are present. Only answer `y' if you trust this file not to put you through a blender. If you answer `n', you can always look at the variables somewhere within the last 3000 characters of the end of the file, and, if they appear reasonable, say `M-x normal-mode' to process them.

Regards, [Ag] gaynor@rutgers.edu

---

complex phones

Dave Fetrow <fetrow@bones.biostat.washington.edu>
Thu, 15 Sep 88 17:05:14 PDT

In RISKS-7.52, Mike Linnig lists a thought-out critera for dealing with ANI (ability to identify a callers' phone number). That's fine but it was (by necessity) lengthy.

It is getting bothersome that a phone (which was and should be simple to use) is getting a bit complex. An awful lot of functions are being built into a box with audio-only feedback and 12 keys! (a trend is to let conventional touch-tone phones do more rather than adding specialized phones with labelled buttons)

Any one (or 2 or 3) extra functions seem easy to absorb but it's looking like we'll be faced with dozens. Worse still: the options are different from phone to phone.

The risk is the classic "one more feature" risk but applied to a device we all use, many times a day.

-dave fetrow-

ISDN/ANI - What one switch vendor told me

achesley@hqafsc-lons.ARPA (achesley@sc) <Allen L. Chesley>
Thu, 15 Sep 88 10:43:17 edt

Yesterday I happened to attend a full-day seminar given by one of the major switch manufacturers. As I had been reading about the ANI question in RISKS, I took the occasion to ask some questions. Although many of the answers depend on how the local telephone company (telco) implements it, this is what they told me about ISDN (when it eventually arrives.

1. Whether or not a calling phone number is available to the receiver is an option implemented at the switch. Except for calls to emergency services, un-listed phone numbers will, in general, not be forwarded.

2. As part of the features available, the local telco may offer a "blocking" command (pre-fix/post-fix/command button) depending on demand and/or the FCC requirements. This and many other possible features would probably be at added cost, but the telcos have not yet figured out how they are going to tariff them

all.

3. There is an entirely new value-added industry possible under ISDN - remote directory services. A call ariving at Company A could have the information in the "D" channel (which carries the calling phone number) routed to Company B, which could then provide a "customer profile" back to Company A before they answer the phone.

Don't start making plans on cutting out your mother-in law's calls just yet (or of autoforwarding them to the local massage parlor). The ISDN folks did not take extension phones into account when they designed the standards, and until they do you are not likely to see full ISDN capability in your homes. In your businesses yes, in your homes no.

Another point we had questions about, and they could not answer, is what happens to all of those companies (like banks) who now do some business using the touch-tone key pad. Under ISDN, signalling uses the "D" channel, not one of the voice carrying "B" channels. Therefore you cannot listen and capture touch-tones off of the conversation.

Allen L. Chesley

NOTE: This message does not express the offical or unofficial opinions of the United States Air Force, the Department of Defense, the United States Government, nor probably most of the United Nations.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 54

Friday 16 September 1988

Contents

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

CerGro voice mail hacked

Really_From John Sheneman <Peter Neumann <neumann@csl.sri.com><>
Fri, 16 Sep 1988 12:23:47 PDT

"Voice mail user[s?] held up by hackers", by Paul Desmond, Staff Writer

LOS ANGELES -- A wholesale grocer here recently fell victim to a small band of hackers that comandeered the firm's voice-messaging systems and used it to run prostritution rings and pass information about drugs.

The message system problems that have plagued Certified Grocers of California Ltd. (CerGro) highlight a threat to which many unsuspecting users may be vulnerable.

Last October, some of CerGro's roughly 300 voice mail users began complaining that they were unable to access their voice mailboxes because their passwords had been invalidated.

Upon investigation, Michael Marks, CerGro's communications supervisor, discovered that hackers had overcome the security features of the system and

had reprogrammed up to 200 voice mailboxes for their own use. The hackers were accesssing the system using a toll-free 800 number CerGro maintained to let travelling employees call in for messages.

[The article goes on to indicate the mailboxes were being used for data on stolen credit card numbers, cocaine prices, and male and female prostitution rings. CerGro removed the 800 number, and activity diminished. However, someone called to say that unless 10 voice mailboxes were established for their use, the intruders would cause damage. The mailboxes were established, but all subsequent messages were recorded...]

[Source: Network World, 12 September 1988, courtesy of John Sheneman, 8319 Kostner Ave., Skokie IL 60076]

Re: Computer error in vote tallying

FRAKE <andy@vax1.acs.udel.edu>
Thu, 15 Sep 88 12:03:58 EDT

A note was posted regarding a New York Times report of a data entry error in a Delaware election. The fact that 2828 was keyed in instead of 28 is correct; Sam Beard was the recipient of these extra votes and not S.B. Woo. S.B. Woo, the current Lieutenant-Governor, now leads Sam Beard by approximately 80 votes in the democratic primary for Senator. S.B. should be declared the official winner sometime this morning.

Andrew Frake, Academic Computing Support, University of Delaware

---

IEEE approval voting

Don Chiasson <G.CHIASSON@DREA-XX.ARPA>
Fri, 16 Sep 88 11:41:36 ADT

A couple of weeks ago, I voted in the annual election for the IEEE executive. This election has an interesting new procedure: approval voting. In this method, you can vote for as many candidates as you wish. The winning candidate is the one who receives the most votes. This offers a number of fascinating options. For example, you can can vote for the two best candidates, or you can vote against someone by voting for everyone else. I like this more than the Hobson's choice of a simple yes to one candidate.

What I would like to ask is: what can go wrong? For example, someone could alter ballots by marking additional places which would be difficult to detect because the number of votes cast does not have to equal the number of voters. What else could go wrong? What robust safeguards could be put in place?

Don

[Some of the other problems are noted in the Saltman, Hoffman, Nilsson works recently cited, and in the talk by Eva Waskell summarized by Ron Newman -- see RISKS-2.42 (14 Apr 86), also in ACM Software Engineering Notes vol 11 no 3 (July 1986, pp. 14-16). PGN]

Reminder -- ROM is not necessarily nonalterable

Andrew Klossner <andrew%frip.gwd.tek.com@RELAY.CS.NET>
Fri, 16 Sep 88 12:15:46 PDT

> Re: Soviet Space Probe (dcf@ALLSPICE.LCS.MIT.EDU) (RISKS-7.52)
> Apparently, US craft have a "panic" mode that takes over if
> there is some problem ... are the panic commands in ROM so that
> they can never be overwritten?"

I can't answer the question, but note that, for software operating in the occasionally high-radiation environment of space, "being in ROM" doesn't mean "can't be overwritten."

-=- Andrew Klossner (decvax!tektronix!tekecs!andrew) [UUCP]

Colwich Junction (UK, 1986)

Mark Brader <msb@sq.sq.com>
Wed, 14 Sep 88 05:17:54 EDT

A month or two ago, I wrote (RISKS-7.22) describing the Colwich Junction train collision, on which a summary of the official report had appeared in Modern Railways magazine. To summarize briefly, the accident was caused by driver error; a contributing cause was overcomplication of the signal system; and another contributing cause was poor braking. (One person--the other driver--was killed; 32 of about 900 passengers were admitted to hospital. Fair, for a 90-100 mph head-on collision.)

Modern Railways and/or I implied that the reason for the poor braking was that the wheel slide prevention (WSP) system, i.e. anti-lock braking, had acted. Several Risks readers said that this must be wrong, because antilock braking should improve the braking, by keeping the wheel-rail friction static rather than dynamic. [That's not actually obviously true, because the wheel-rail coefficient of friction must be closer to the coefficient of friction within the brakes in a train than are the corres- ponding values in a car. And static friction at one place implies dynamic at the other. But it seems probable that WSP should improve braking.]

I have now obtained further information, including the official report (thanks, Clive Feather!). But the principal points (no pun intended) remain obscure.

First, I should point out that the WSP systems on British trains are not actually designed to minimize the stopping distance. They are installed to stop wheelslip for two *other* reasons:

- If a wheel slips during acceleration, it can spin so fast that the frictional heat will damage both wheel and rail surfaces.
- If a wheel locks during braking, it will develop a flat spot,

requiring its surface to be reground.

The general principle is to compare speeds of different axles, and assume slipping if they differ by more than some threshold. This obviously makes the assumption that slipping wheels will slip unequally, which may not actually always be true in the case of braking.

According to the official report on a different accident, the typical coefficient of static (non-slipping) friction between rail and wheel on a dry day is 0.3, and on a wet day 0.2; 0.1 suffices for normal braking, and 0.05 to prevent overrunning of signals (assuming no driver error). The last two figures may vary from one line to another, and thus not be exactly right for the Colwich Jct. area. Values worse than 0.05 occur only in conditions such as heavy falls of leaves, or icing.

The unexplained part is this. All witnesses agreed on the speed of the train. The driver and the other man in the cab agreed on where the brakes had been put to emergency. A witness heard a repetitive air sound coming from several cars, indicating that the WSP was operating and therefore that the brakes were indeed on hard. But all witnesses also agreed that the train decelerated more gently than in emergency braking. The investigating officer made a considerable number of tests, and reproduced the actual stopping distance only by driving the train about 10 mph faster than everyone said -- and running the test on wet track, when on the day of the accident it was dry!

The WSP operates independently on every car, so multiple failures tending to apply "too much protection" are not plausible. Actually, some of the surviving WSP units did have faults in that direction, but not enough of them to explain what happened.

The report's conclusions and recommendations read in part:

Suffice it to say that I am satisfied that [the driver], once he
realized that he was about to run past Signal CH23 at Danger,
made a full emergency application of the brakes and there is no
substantial evidence to show whether or not the brakes operated
within the normal limits of efficiency. ...

It is impossible to determine to what extent the operation of the
wheel slide prevention equipment or any other factor reduced the
efficiency of the braking, but there is no doubt that it was
reduced to a certain extent.

Notice that this leaves ambiguous whether it was reduced by the WSP or by something else. This is the report of an investigator who is stumped!

A full emergency application of the brakes is likely to introduce
wheel slide, even on dry rails, particularly if adhesion is reduced
by any contaminant,

(One might guess that *that's* the answer, but there was no evidence.)

and thus activate the wheel slide prevention

equipment where fitted. Full emergency brake applications ... are
made ... almost inevitably only when there is a true emergency.
A very small distance may make all the difference ... and thus with
the full emergency application of the brakes I believe that all
brakes should be fully applied, even if wheel slide does occur
and wheel flats are made on the wheels. I recommend, therefore,
that consideration should be given to the fitting of equipment
to automatically eliminate the operation of wheel slide prevention
equipment in the event of an emergency brake application being made.

In short, the investigating officer, Major P. M. Olver, does not appear to have considered the matter of static and dynamic friction; or perhaps Olver is concerned more with the possibility of the WSP acting "by mistake" due to a problem with it, but does not state this explicitly. One wishes that in addition to trying to reproduce the accident, the test runs had included some with the WSP disabled. The effect of that on the stopping distance would have been highly germane to the recommendation of overridable WSP.

By the way, there have been several letters about the accident in Modern Railways, but all commenting on the (pun coming) signal aspect. Perhaps I'll write a letter about this point myself.

Mark Brader

Smoke Inhalation on Amtrak's "Crescent"

Mike Trout <miket@brspyr1.brs.com>
15 Sep 88 17:35:00 GMT

Taken without permission from _The_Call_Board_, publication of the Mohawk & Hudson chapter of the National Railway Historical Society, which in turn took it from _Callboy_ of the Massachusetts Bay chapter, which in turn took it from _The_470_ of the Portland chapter:

"About 125 children and 30 adults suffered from smoke inhalation after someone pulled the emergency brake cord on Amtrak's "Crescent" while it was in a tunnel near Washington Union Station on May 12, sending exhaust fumes spewing into the cars. The "Crescent" departed Washington southbound with two engines, 16 cars, and about 400 passengers and 18 crew aboard. Five minutes later, as the train was in the tunnel, an unknown person for unknown reasons pulled the emergency brake. The train stopped in the tunnel with its emergency brakes applied, and the second engine stalled or died. The train crew, thinking that an air hose that controls the brake system had parted, walked the train looking for such a problem. Finding none, the crew searched the cars and found that the emergency brake handle in the first car had been pulled. Unable to release the brakes, the crew shut down the lead engine. Trains that leave Washington Union Station going south immediately enter a 3,900-foot tunnel that roughly goes under the grassy Mall stretching form the Capitol to the Lincoln Memorial. Another Amtrak engine pulled the train back to the station, and buses retrieved the passengers from the hospitals to take them to hotels for the night."

Would it not be fairly simple to install sensing devices in locomotive

cabs, indicating when an emergency brake handle had been pulled? If the crew knew at once the cause of the automatic brake application, they would not have wasted time looking for broken air hoses. And why, upon finding the real cause, was the crew unable to then release the brakes? Emergency brake systems have been around for many, many decades. One would think that they would have been "perfected" by now. Comments from railroading experts?

Michael Trout UUCP:brspyr1!miket
BRS Information Technologies, 1200 Rt. 7, Latham, N.Y. 12110 (518) 783-1161

Computer assigned hotel rooms

Bruce Wampler <wampler@unmvax.unm.edu>
Wed, 14 Sep 88 19:20:26 MDT

I have also had the experience of getting occupied hotel rooms mixed up by a clerk or computer, but which revealed a true software problem in the hotel's billing system.

My wife and I had just arrived in LA from a 19 hour flight from Fiji, and missed my connection, so was jet lagged. The clerk gave us the key for room 456, but apparently entered 546 into the machine (as I found out the next morning.) 456 was unoccupied, so I didn't have any problem at the start. Unfortunately, about 3 a.m., someone else was assigned to 456 and woke us up. The dead bolt kept them out, but it sure messed up what little sleep we were getting.

When we first arrived, we made several long distance calls that we expected to be billed to the room. Well, when we tried to pay the next morning, there was no bill. Since the computer listed 456 as empty (the 3 a.m. person was assigned another room, we were told), then there was no provision for recording phone calls. I would have preferred the sleep, but at least we got free phone calls for the trouble. However, the hotel lost revenue because the billing software didn't account for phone calls from empty rooms. I suppose if the staff knew that, they could take advantage.

Bruce Wampler

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 55

Saturday 17 September 1988

Contents

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

The Ethics of Conflict Simulation (Re: RISKS-7.49)

Mike Trout <miket@brspyr1.brs.com>
16 Sep 88 16:23:05 GMT

In RISKS-FORUM 7.49, Eric Postpischil and Henry Spencer disagree with Ed Nilges' assertion (in RISKS-FORUM 7.45) that increasing technical abilities of computer games has corresponded with a decline in social and moral content. They point out the subtle yet insidious context of chess and _Monopoly_, the large number of computer games that encourage moral behavior, and the overt content of standard wargames.

Although many of their points are valid, I must disagree with the basic contentions of Eric and Henry. I, too, have noticed the same disturbing trend aptly noted by Ed.

I have been involved with the design, use, and history of wargames (perhaps

more correctly called "conflict simulations") for nearly 20 years. Over that time, I have witnessed a definite change in attitude among those in the field. In the mid 70s, a major debate erupted over whether the industry leader should or should not do a proposed project for the Pentagon. The consensus was that dealing with the Pentagon would poison the intellectual atmosphere that had so far kept conflict simulations a model of integrity. The project was never done.

Shortly thereafter, the industry leader was destroyed in a hostile takeover attempt, and surviving companies began the first Pentagon projects. Today, most wargaming companies fight for those precious Pentagon dollars, and gaming has suffered for it. Many simulations are today designed for the purpose of developing better ways to slaughter people, rather than as intellectual history lessons. Worse, there is a disturbing tendency to design simulations as vehicles for displaying aggression. Certainly 20 years of progress has given us conflict simulations that are technically far more accurate than anything done in the "Golden Years" of the 60s and 70s, and the use of computers in simulations has revolutionized the industry. But with the improvement in technical accuracy and mechanics has come a change in the purpose of wargames. Instead of serving primarily as learning tools, they are now approached as pure profit-making ventures, military aids, or macho exercises. The "learning tool" aspect is still there, but it has been subverted by baser instincts.

Of course, there is the "fun" aspect of conflict simulations. Even the most intellectual simulations invariably contain certain amounts of "fun," and most of us get a great deal of satisfaction that way. I would not deny that I myself have enjoyed watching my Soviet infantry turn a Nazi pillbox into a fireball. Yet when that enjoyment becomes the PRIMARY purpose of the simulation, something is wrong. This is one of the more disturbing aspects of many arcade-type computer games. It doesn't matter whether you are pushing a button on a joystick, typing in a line of commands, or moving a cardboard counter across a map. What are the functions of the simulation? I submit that greed and aggression have no place in the study of a human activity which is itself intrinsically rooted in greed and aggression.

Michael Trout (miket@brspyr1) =-=-=-=-=-=-= UUCP:brspyr1!miket
BRS Information Technologies, 1200 Rt. 7, Latham, N.Y. 12110 (518) 783-1161

Re: Social content of video games (RISKS-7.49 etc.)

Tim Wood <mtxinu!sybase!linus!tim@ucbvax.Berkeley.EDU>
Wed, 14 Sep 88 19:28:23 PDT

The conditioning effect of violent video games should be at least as much of a concern as the effect of similar content on viewers of ordinary TV. Video games do not present the spare, tokenized arena of chess or Monopoly; they present a (speculative) graphical scene of the player's struggle toward the goal. When the player and the obstacles are cast in demeaning human stereotypes, the game is degrading to play. The key aspect of video games is the explicit graphical interface that requires the player to focus on the images of the game's creators rather than create his/her (possibly less hostile in some cases) own mental images.

{ihnp4!pacbell,pyramid,sun,{uunet,ucbvax}!mtxinu}!sybase!tim

Voluntary disclaimer: This posting is solely my personal opinion.
It is not a representation of Sybase, Inc.

---

re: Credit Doctors

Dave Robbins <dcr0%uranus@gte.com>
Fri, 16 Sep 88 14:40:04 EDT

donn@cs.utah.edu (Donn Seeley) quotes in Risks 7.50 portions of the Newsweek article about credit doctors. The concluding question is:

> Are credit bureaus' security measures really this lax? It's not hard to believe, just appalling.

I have a couple of comments to add:

1) This type of activity is not uniquely a computer risk. I can imagine a computerless credit bureau, where records are kept on paper, and further imagine a 'credit doctor' fraudulently obtaining the credentials necessary to gain access to the credit bureau. The 'doctor' then calls up the credit bureau and obtains the desired information. The difference, of course, is that in this case the 'doctor' is probably dealing with a human at the credit bureau, and this human might by some chance figure out that the 'doctor' is up to no good.

2) The computer-related risk is, of course, that this sort of activity is much more likely to happen with computerized credit bureaus. The volume of information involved, and the anonymity of the individual making the request for credit information (via a terminal) make it much more difficult for requests to be validated and for fraudulent usage to be detected. This is just one more example of a well-known risk that is all too often not accounted for in the design of a system.

3) Surely there must be a reasonable way to provide legitimate access to credit information without making it so easy to obtain illegitimate access! As the credit bureaus operate today, any individual who knows how to access the credit bureau's computer can apparently locate anyone's credit information. It has been demonstrated that we cannot place much trust in those individuals at the banks, etc. who have access to the credit bureaus. I can imagine an individual whose credit information is on file at the credit bureau providing a unique 'password' to the bank for the purpose of a credit check, but how then is that password protected from abuse? (I seem to remember a proposal for a relatively secure version of this sort of thing in CACM 3-4 years ago.) Or is this an inevitable and unavoidable risk of having computerized records? I should hate to think so -- it might lead me to advocate keeping computers away from such sensitive records.

These issues are not really new, so I think I'll stop at this point,

and wait for the next creative abuse of computerized personal records
to pop up in the news.

Virus in ROM on commodore 64

Jurjen N.E. Bos <jurjen@cwi.nl>
Sat, 17 Sep 88 12:06:45 +0200

The commodore homecomputer has an EPROM containing the boot and basic software.
This ROM is in principle programmable only if the programming voltage is
applied. In practice it is possible to modify the ROM by writing to it many
times. This already caused a severe problems because a crashing program
destroyed the ROM in a computer of a friend of mine. I do not know if there
already is a ROM virus on the 64, but I'm sure it is possible. This makes
those computers more vulnerable to viruses than any other homecomputer.

Re: Destructive remote controls

<attcan!utzoo!henry@uunet.UU.NET>
Sat, 17 Sep 88 00:26:17 EDT

> REMOTE WILL DAMAGE your home TV sets."

I'd say they're just trying to scare you. I find it hard to imagine a remote
control that puts out enough infrared to even be competitive with direct
sunlight -- and any consumer product must be designed for the possibility of
lengthy periods of direct sunlight.

Henry Spencer at U of Toronto Zoology

Damage by remote controllers

Jurjen N.E. Bos, CWI, Amsterdam <jurjen@cwi.nl>
Thu, 15 Sep 88 10:49:16 +0200

Talking about TV sets that are claimed to be damaged by remote controllers...
I happened to go to Disneyland lately where I saw the 3D movie "captain EO".
As you might know, this 3D effect is done using a special kind op polaroid
glasses. They said after the movie was over:
"Please do not take these glasses as a souvenir.
They will impair your vision outside this theatre."
There they go again! What's the difference between this theatre and the outside
world? Those glasses will either impair your vision on the long run (which I
doubt) or they won't. The only difference between the inside of the theatre
and the outside world is the 3D illusion they make.

-- Jurjen N.E. Bos

[Irrelevant to computers, but nevertheless interesting
as another example of the same approach! PGN]

Another one-key mishap

Russ Nelson <nelson@sun.soe.clarkson.edu>
Fri, 16 Sep 88 11:12:20 EDT

When I worked at HP, we acquired a new HP-IB hard disk drive with integral tape backup. To perform a backup or restore, you simply pull off the faceplate and press disk-to-tape or tape-to-disk. Both switches were identical, and you can guess what eventually happened...

[As you might guess, there are about 12 messages pending on variants of "rm" pitfalls and other single-keystroke fiascos. We'll slow down on these for a while. PGN]

Re: ISDN/ANI - What one switch vendor told me

Edwin Wiles <ewiles%netxcom@uunet.UU.NET>
Fri, 16 Sep 88 17:19:43 EDT

In RISKS 7.53 <Allen L. Chesley> Writes:
> Another point we had questions about, and they could not answer, is what
> happens to all of those companies (like banks) who now do some business using
> the touch-tone key pad. Under ISDN, signalling uses the "D" channel, not one
> of the voice carrying "B" channels. Therefore you cannot listen and capture
> touch-tones off of the conversation.

I'm not absolutely certain that we are talking about the same thing, but "Feature Group D" services do indeed allow you to capture touch tones off of the conversation. (I have worked with this, so I know something about it.)

The ANI signalling *is* done on different lines from the ones that carry the conversation, and uses something other than DTMF. However, once the ANI signalling is done, the receiver of the call performs an "Acknowledgement Wink" on the special line. This opens the 'voice path', which is what carries both the conversation, and any additional touch tones the caller sends. (Such as a command code to tell the bank what to do with your account.)

The RISKY thing about this setup, is that it takes an additional "Wink" to 'accept' the call. Theoretically, you could complete your entire conversation without sending that wink, and never be billed for the call since the telco doesn't start billing until the call is 'accepted'. Practically, if you did it much, the telco would notice, and you would be "up the evil smelling tributary, with no visible means of locomotion, and no knowledge of aquatics."

The reason for this setup is so a service can extract further addressing information before the caller is billed. This prevents a caller from being billed for a call which cannot be completed.

DISCLAIMER: I do not work for any telephone company.
Neither I, nor my company, condone any illegal actions.

Edwin Wiles, NetExpress Comm., Inc., 1953 Gallows Rd. Suite 300 Vienna, VA 22180

Call for Papers, Invitational Workshop on Data Integrity

"RUTHBERG, ZELLA" <ruthberg@ecf.icst.nbs.gov>
16 Sep 88 17:39:00 EDT

CALL FOR PAPERS
Invitational Workshop on Data Integrity
January 25-27, 1989

Sponsored by and Held at
National Institute of Standards and Technology
(formerly National Bureau of Standards)
Gaithersburg, Maryland

The National Institute of Standards and Technology is sponsoring an Invitational Workshop on Data Integrity to be held at NIST in Gaithersburg, Maryland on January 25-27, 1989. The Workshop will focus on the concepts of data integrity and data quality, and the characteristics, metrics, and principles needed to define and provide a suitable framework for data integrity and data quality.

This invitational workshop is a follow-on to the October 27-29, 1987 invitational Workshop on Integrity and Privacy in Computer Information Systems (WIPCIS). The latter originated as a response to a paper by Clark and Wilson presented at the IEEE Security and Privacy Conference in April, 1987. That paper compared commercial and military computer security policies. The 1987 Workshop focused on commercial sector interpretations of the issues of Assurance, Granularity and Function, Identity Verification, Auditing, and System Correspondence to Reality and related these to a data integrity model.

A subsequently-formed data integrity working group of the NIST Computer and Telecommunications Security (CTS) Council has proposed definitions for data integrity and data quality. These have been incorporated, along with other conclusions, in a paper written by the working group chair Robert H. Courtney, Jr. It is intended that this paper serve as a strawman to stimulate responses in the form of papers to be given at the January Workshop. The Clark & Wilson paper would form an example within this framework. Although computer and telecommunications system integrity is broader than data integrity, consensus findings about data integrity would contribute significantly to our understanding and handling of the broader concerns of integrity.

Papers are being sought from the computer security community for presentation at the Workshop. Papers could address but need not be limited to the following topics:

- Key principles for achieving data integrity.
- Key principles for achieving data quality.
- The application of principles to achieve integrity and quality of data.
- The attributes of data quality (other than accuracy, timeliness and completeness).

- o Is confidentiality an attribute of data quality?
- o Connection between Quality Assurance and data integrity.
- o Connection between Quality Control and data quality.
- o Relation between data quality and the value of data.
- o Organization-specific data integrity/data quality policies derived from a body of principles.
- o Cost-Benefit Relationships between security controls and data quality and integrity.
- o Organizational structures for assigning data integrity, quality assurance, and data quality functions.
- o A realistic internal audit role relative to data integrity and quality.
- o A reasonable external auditor role relative to data security and its subset data integrity.
- o The relation of people roles (ADP staff, user, internal auditor, quality assurance, quality control) to data integrity and quality.

Papers should be submitted by November 17, 1988 to:
National Institute of Standards and Technology, Computer Security Division,
Attn: Zella Ruthberg, A-216 Technology, Gaithersburg, Maryland 20899

Approximately six papers will be selected for presentation and discussion. Selections will be made by December 7, 1988.

The strawman paper will be sent on request. For further background, people may also request a copy of the report of the 1987 WIPCIS workshop. The paper and report are available from Robin Bickel at the above address or 301-975-3359.
For further information on the Workshop contact Zella Ruthberg at 301-975-3361.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 56

Wednesday 21 September 1988

Contents

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

Runaway mouse problem in popular commercial WP program

Jon Jacky <jon@june.cs.washington.edu>
Mon, 19 Sep 88 09:17:04 PDT

From COMPUTERWORLD, Sept. 5, 1988, p. 39:

MICROSOFT SCRAMBLES TO HEAD OFF RUNAWAY MOUSE WITH WORD REWRITE -Steven Jones

Users running Microsoft's Mouse and Word 4.0 software program on IBM Personal System/2 computers have inadvertantly sent Mouse on a wild spree by hitting an uncommon combination of keystrokes and clicks. The results include a variety of unwanted windows being opened and system freezes wherer the user cannot get into the command line. "It goes a little nutty," said Jeffrey Sanderson, Microsoft's group product manager for word processing.

Microsoft said that, with the help of IBM, it determined the problem to be with the PS/2's mouse port when the mouse was used to point and click with Word. Sanderson said the problem was spotted last February when users started to complain about the wild mouse.

In all, Microsoft received about 200 calls from users that had an encounter with the rowdy device. Microsoft made a slight modification to Word to quiet Mouse and began shipping the new version, called Word 4.00A, in May.

While Microsoft said that Word was the only part of its application software line that experienced the problem, one user said he had similar difficulties when running Xerox Corp.'s Ventura Publisher. ...

- Jonathan Jacky, University of Washington

Wrapping Britain round the Greenwich meridian

Jack Campin <jack@cs.glasgow.ac.uk>
19 Sep 88 15:20:36 GMT

A point related to the discussion about averaging angles is made by John Lamb in the article "The everyday risks of playing safe" in New Scientist (8 Sept 1988). Describing the software used for air traffic control in the London area by the Civil Aviation Authority on its IBM 9020 machine he writes:

> "One of the more startling problems concerned the program's handling of the Greenwich meridian. The National Airspace Package, designed by IBM's Federal Systems division, contains a model of the airspace it controls, that is, a map of the airlanes and beacons in the area. But, because the program was designed for air traffic control centres in the US, the designers had taken no account of a zero longitude; the deficiency caused the computer to fold its map of Britain in two at the Greenwich meridian, plonking Norwich on top of Birmingham."

Jack Campin, Computing Science Dept., Glasgow Univ., 17 Lilybank Gardens, Glasgow G12 8QQ, SCOTLAND work 041 339 8855 x 6045; home 041 556 1878

Crime and (indifferent) Punishment

Glen Matthews <CCGM%MCGILLM.BITNET@CORNELLC.CCS.CORNELL.EDU>
WED 21 SEP 1988 08:15:00 EDT

In the Montreal Gazette (Tuesday Sept. 20 1988) a report appeared that rounded out the story some months back re a Quebec firm selling welfare information illicitly obtained as a result of co-operation of government employees. Criminal charges against those involved were not laid due to a decision by Crown prosecutors in May. However, the two civil servants (by their actions I'd say most "uncivil" servants!) involved pleaded guilty to a violation of Quebec's welfare act when they gave out confidential information on welfare recipients.

According to the report, they were traced by using "security devices built in to the computer system". It goes on to say that "each government employee has a computer code, which automatically is logged on all files he calls up".

The two were fined $100. Government officials have refused to say what punishment the provincial government, their employer, has meted out. Possible measures range from an oral reprimand, a note in the employee's suspension, or firing. Had they been fired, I'd assume that this would have been stated.

So, computer crime in Quebec, while perhaps not rewarded, is treated with little urgency. With such a lenient approach to malefactors, I wonder what other things are going on; certainly, this case provides no deterrent to future "hi-jinks".

Glen Matthews, McGill University

Software Mixup on Soyuz Spacecraft

Karl Lehenbauer <karl@sugar.uu.net>
Wed, 21 Sep 88 8:00:04 CDT

According to Aviation Week (September 12, 1988, page 27), the second failed reentry of the Soviet Soyuz-TM spacecraft on September 7, the engines were shut down within seconds due to a computer problem: "Instead of using the descent program worked out for the Soviet-Afghan crew, the computer switched to a reentry program that had been stored in the Soyuz TM-5 computers in June for a Soviet-Bulgarian crew. Soviet officials said last week that they did not understand why this computer mixup occured."

The article notes that the crew was committed to a reentry because they had jettisoned the orbital module that contained equipment that would be needed to redock with the Mir space station.

The article also noted that Geoffrey Perry, an analyst of Soviet space activities with the Kettering Group, "said the crew was not flying in the same Soyuz that they were launched in, but instead were in a spacecraft that had been docked with the Mir for about 90 days. He said that is about one-half the designed orbital life of the Soyuz."

-karl

RISKS of (Suspected) Crooks Running Dinosaur-DOS

"F.Baube" <fbaube@note.nsf.gov>
Wed, 21 Sep 88 10:43:07 -0400

The WashPost (Mon Sep 19) had a story on the procurement investigation.

"Sometimes, however, investigators hit unexpected roadblocks. In a search of consultant James Neal last June, for example, FBI agents seized computer disks

only to find they couldn't run them on the agency's computers. So they subpoenaed Neal's vintage machine, gently suggesting in the subpoena that he might be kind enough to help the FBI agents by demonstrating how it works.

When Neal sought to have the subpoena quashed, [the judge] ruled that the government could have the computer for five working days. But, he added, "I don't understand a subpoena asking for assistance. The government will have to learn to work the machine itself."

#include <disclaimer.h>

Multiple reservations and single bills

Markus Stumptner <mcvax!tuhold!markus@uunet.UU.NET>
Mon, 19 Sep 88 20:06:54 -0100

This is an article which appeared a few weeks ago in recs.arts.sf-lovers.
It shows a case where, even after the error had become known, the hotel staff were unable to correct it.

I have not attempted to verify the story. Only the hotel name was changed to protect the incompetent.

(P.S. No mention is made in the article of a computerized reservation system. After reading it, however, I rule out the possibility of unsupported humans botching it this bad.)

Markus Stumptner, Technical University of Vienna, Paniglgasse 16,
A-1040 Vienna, Austria UUCP: tuvie!tuhold!markus

= =

From: GWCHUGPG@uiamvs.BITNET (Jacob Hugart)
Newsgroups: rec.arts.sf-lovers
Subject: Conventions and Hotels
Message-ID: <8808261600.AA12810@rutgers.edu>
Date: 26 Aug 88 16:00:22 GMT

Hotels, Conventions, and People don't mix.

Here's a horror story for you.

A good friend of mine, Jordan Orzoff, is a gamer. Not a geek, but a devoted role-player. Anyway, he was going to GM a game at GenCon/Origins, based upon a scenario he used on some of his friends. Because he was going to judge a game, he got his judge's pre-registration packet early. This came with a hotel reservation form which he filled out and listed me as a roommate.

We received our confirmation from the <XYZ> Hotel (our first choice) and from GenCon. Great, no problem.

When we arrived in Milwaukee, Wisconsin, we went to the <XYZ> and asked

about our room. The desk person said that no rooms were available now, but a reservation for Nathan Orzoff and Jacob Hugart was listed.

Here's where the fun begins. Jordan has a well-know cousin named Nathan Orzoff, who is well-known in some gaming areas, and whom Jordan had never met. We asked the desk person if there was another Orzoff listed, and he said no. He also said he'd change the first name. Jordan said he probably shouldn't, Nathan might show up. In any case, we couldn't check-in until 3pm.

We arrive at 3pm. Jordan gets in line. After a bit, he calls me up and introduces me to his cousin, Nathan. Nathan and a friend had also reserved a room at the <XYZ> for GenCon. Unfortunately, I had a reservation with Nathan and Jordan had a reservation with Nathan's friend. All four of us were placed in the same room, with one double-bed.

Since Jordan and I had our <XYZ> confirmations, we got the room right away, and Nathan and friend got one too, after a bit. Jordan payed his downpayment with Visa, I with American Express.

After four days, when GenCon was over, Jordan and I had to check out. He had received two bills, one for him, one for me. When we looked closely at the bills, both of them had Nathan Orzoff's address on them, and mine had my name as "Jordan, Hugart" whereas Jordan's was "Orzoff, Jordan." So now we have five people in this room, according to the reservations: Jordan Orzoff, Nathan Orzoff, Nathan's friend, me (Jacob Hugart), and Hugart Jordan.

All reserved and billed in the same room with one double-bed.

Since the bills had a "Balance Due" line, we went to the desk and said we'd like to check out and pay our bills. The person at the desk looked up our account on the computer, and said we were already checked out. News to us. Also, our bills had been paid in full. More news. The desk person showed us the receipts we had signed. Fine.

Jordan has a theory. He believes Nathan got stuck with our bills, and paid them. That would explain how we checked out before we checked out. But it doesn't explain why one bill would be paid on AmEx, the other on Visa.

I liked the <XYZ>. But I wouldn't trust their reservation system as far as I can spit it.

<ruffwork@edison.cs.orst.edu>
Wed, 21 Sep 88 14:07:33 PDT

This is via Kaj Wiik in Finland (he is an associate of Gilbert Leppelmeir). It is reprinted with permission (I suggest people try to get permission, it's not only the "correct" way to do it, but it can also be fun! Right, Eugene?).

It was such a twisted set of "coincidences" it could only happen in real life. From this note the following questions come to mind:

- the probes are programmed "real time" ?

- they are programmed in a very low level language ?
- the code isn't verified before transmission ?
- there is no continous telemetry from the probe ?
- there is no "sanity check" in the probe, and no "panic" mode (as several have told me NASA uses) to keep the probe from doing really dumb things ?

At least the "hopper" is on Phobos 2 instead of Phobos 1...

--Ritchey Ruff ruffwork@cs.orst.edu -or- ...!tektronix!orstcs!ruffwork

------- Forwarded Message

Return-Path: @cunyvm.cuny.edu:kwi%kolvi.hut.fi@santra.hut.fi
To: ruffwork@mist.cs.orst.edu (Ritchey Ruff)
Date: Wed, 21 Sep 88 17:06:21 EET DST
From: Kaj Wiik <kwi%kolvi.hut.fi@cunyvm.cuny.edu>
Subject: Re: Soviet Mars probe PHOBOS 1 communications lost enroute

No problems, you can publish the notes. There were some inaccuracies in the original posting concerning the author, so could you please publish the following, corrected version.

Kaj Wiik kwi@kolvi.HUT.FI kwi@finhutee.bitnet

= =

Phobos I news
Gilbert W. Leppelmeier 12.9.88
VTT (Finnish Technical Research Centre),
Instrument laboratory

At the last session of the meeting of the International Science Committee of the Spectrum-X-Gamma project, Friday, 9.9.88, Prof. R. Sagdeev gave a presentation of "all we know at present about what has happened to Phobos I". These are my notes from that presentation. (Not an official IKI announcement)

A few weeks ago it was decided to move the control of Phobos I from the Crimean Space Center to a Center near Moscow. Among other things, this involved using a new computer with a different keyboard. Traps were installed in the new operating system to catch characteristic operator errors, including one wherein an operator now had to insert a particular character at the end of a command. If he failed to do so, a reminder would come on the screen asking him if he had forgotten to do so, and the computer would not continue unless the character were included, OR the operator specifically overode the computer.

On 29.8.88 a very long message was being prepared for

transmission to Phobos I. At one point, near the end of the message, the operator failed to add the character, the computer stopped, but failed to display the question on the screen. The operator thought it was a computer error and overode the stop. The absence of the particular character changed the bit pattern of the following instruction, into a bit pattern, not on the list of accepted commands, but which did call an area of the onboard ROM which had a list of possible commands, used in development and left there for possible future use. Unfortunately, the particular pattern created in this error translated into turning off the attitude control thrusters.

Two days later the Control Center sent a message to Phobos I and received no answer. It is now believed that as the spacecraft slowly changed orientation it lost power, because the solar panels no longer faced the sun, and everything turned off. The serious concern is that many items [from private conversations I gather both in spacecraft support and instruments] need electrical power to avoid becoming too cold, and will be permanently damaged if they get too cold.

Sagdeev listed the following points as links in the chain:

- error on operator's part
- computer failure
- operator decision to circumvent computer
- absence of cross checks
- actual command sent able to enter ROM
- The OB computer must be programmed to prevent suicide. [I believe RS said the OBCPU was 8-bit. You can't do much checking with such a small cpu on such a large spacecraft.]

This is the first failure of a Soviet deep space spacecraft since 1972.

Added 14.9: This is what I wrote when I returned from Moscow. Looking at my notes, I realise that the move of control center may have taken place on 29.8 and the transmission error later.

------- End of Forwarded Message

`Computer programmer convicted of creating "virus"'

<linnig@skacsl.csc.ti.com>
Tue, 20 Sep 88 20:56:26 CDT

From 9/19/88 Ft. Worth Star-Telegram

A 40-year-old computer programmer was convicted last night of deliberately creating a computer "virus" -- a series of destructive programs, one of which was used to delete records from his company's computer within days after he was fired.

A Tarrant County jury deliberated about six hours before convicting Donald Gene Burleson of harmful access to a computer with valued loss and damage of more than $2,500.

Burleson's trial was considered a landmark case because he was the first person tried under a 1985 Texas law prohibiting computer sabotage. It also may have been one of the first such trials in the nation, trial Judge John Bradshaw told jurors after the verdict.

Prosecutor Davis McCown said the verdict proves that computer crime is not impossible to prosecute.

"The jury heard the evidence and did what they felt was best," McCown said. "This proves it is not an unprosecutable offense. It may be hard to put a case together, but it's not impossible."

Burleson, of Irving, is scheduled to be sentenced this morning by Bradshaw, a retired state district judge who presided over the nine-day trial in Impact Court II in Fort Worth.

The third-degree felony of which Burleson was convicted carries a possible punishment of two to 10 years in prison and a fine up to $5,000. As a first-time offender, Burleson is eligible for probation.

Burleson already has lost a $12,000 civil lawsuit to USPA & IRA, the Fort Worth security brokerage and insurance company for which he worked until he was fired for unrelated reasons Sept. 18, 1985, just days before company officials discovered that 168,000 records of sales commissions had been deleted from their computer system.

The computer virus was discovered by USPA & IRA employees as they worked feverishly to restore the records, which were deleted sometime after 3 a.m. Sept. 21, 1985, witnesses testified.

Although hundreds of computer records and other documents were introduced during the trial, the main issue became the credibility of key witnesses, including Burleson and Duane Benson, a USPA & IRA senior programmer analyst who unraveled the destructive scheme he said was traced to Burleson.

Benson, who spent four days testifying about how he uncovered the scheme, said the destructive programs were created Sept. 2 and Sept. 3, 1985, on Burleson's computer terminal by someone using Burleson's computer password.

The automated virus series, which was designed to repeat itself periodically until it destroyed all the records in the computer system, never was automatically activated, Benson said. Instead, someone manually set one of the programs in motion Sept. 21, deleting the records, then covering his tracks by deleting the program, he said.

But Burleson and a computer expert he hired contended that the virus and the related delete program could have been created by someone else using Burleson's terminal and password.

Burleson contended that he and Benson did not get along and that Benson created the destructive programs to make Burleson look bad and Benson look good when he restored the damaged system.

Prosecutors contended that Burleson, who had been fired, had more motive to destroy the records than did Benson, to whom Burleson confessed the sabotage a week after it was discovered, according to Benson's testimony.

But Burleson's alibi was his undoing, one juror said.

Burleson testified that he was more than 300 miles from Fort Worth on Sept. 2 and Sept. 3, and he produced a Texaco credit card receipt he said proved he had a tire repaired in Rusk on Sept. 3, on his trip home from Jasper. His son, father and former wife supported his alibi.

But Burleson school attendance records show that Burleson's son was in school Sept. 3, not traveling with his father. A Texaco official said the receipt Burleson produced was printed October 1987, two years after the alleged transaction. And USPA & IRA records showed Burleson attended a staff meeting Sept. 3.

"Three or four days ago, I was absolutely convinced he was innocent," juror Randal Scott Owen of Fort Worth said last night after the verdict. "But I feel he fabricated stories about his alibi. That just destroyed his credibility with us.

"He didn't have the burden of proof, but he should have shrugged his shoulders and said, "I'm innocent and I have no proof,' " instead of fabricating evidence, Owen said.

Eleven other jurors declined to comment before leaving the courtroom. And Owen acknowledged that the trial was hard on everyone.

"I have a real problem sending someone to jail for a white-collar crime," he said.

Burleson also declined to comment after the verdict, sitting slumped at the defense table as his attorney, Jack Beech, gave media interviews.

"I was sort of surprised," Beech said. "I had expected a better verdict. We'll have to wait until after the sentence to decide whether we want to appeal."

[Of course, it was a time-bomb, not a virus. But then so were many of the other so-called viruses. By now the popular press have completely perverted both "virus" and "hacker", but in any subsequent RISKS discussions, let's try to rise above that. BTW, I received shorter versions from Steve Smaha and Henry Cox, but in this case decided to go with the long one, for the possible interest of those of you whose local papers truncated. PGN]

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 57

Saturday 24 September 1988

Contents

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

Faulty locks delay prison opening

Henry Cox <cox@spock.ee.mcgill.ca>
Thu, 22 Sep 88 19:59:46 edt

LOCKS THAT WORK ARE KEY TO OPENING OF NEW JAIL
Montreal Gazette, 22 Sept 1988

Placerville, Calif. (AP) - The new El Dorado County jail would be ready to open except for one problem: the cell doors won't lock. Faulty electronics have affected the high-technology locks, along with television monitors and a communication system, jail commander Ed Newman said. "These are very dramatic problems," said Newman, adding that 13 flawed electronic panels are "literally the hands and feet of the officers." The panels have been shipped to a Maryland electronics company to be reworked and won't be back for three weeks.

The jail's design relies on a central control post from which guards can electronically open and close cell doors, communicate with prisoners and operate lights. The jail's contractor is paying a daily penalty of $1250 to compensate for the delays, county general services director Joe Winslow said.

[Kidding aside, one hopes that the jails designers were/are aware of the risks inherent in such a centralized system. Perhaps we ought to mail them a few back issues of RISKS.]

> [Don't kid yourself. There are equally nasty risks with distributed control. PGN]

In the future, risks of purchasing handguns

<ark%asgard@CS.RIT.EDU>
Thu, 22 Sep 88 09:24:02 EDT

An excerpt from Time Magazine, September 26, 1988, p. 26.

> "Why Wait a Week to Kill? The gun lobby
> overwhelms an attempt to restrict handguns."

[...The article begins with a description of the Brady Amendment that would have required gun dealers to wait seven days before completing a handgun sale, so police could do an identity check on the purchaser. The National Rifle Association lobbied hard against the amendment, and the House of Representatives defeated it, 228 to 182. Now for the computer risk...]

"Florida Republican Congressman Bill McCollum Jr. offered a way out of the quandary. He proposed replacing the waiting-period requirement with a provision to give all 275,000 federally licensed gun dealers in the U.S. instant access to a nationwide list of convicted felons. Prospective gun buyers could be fingerprinted and the samples sent electronically to Washington for an instantaneous check against the FBI's millions of prints.

"But there is no master list of convicted felons, no way to make such data quickly and widely available, and no speedy means of sending and matching fingerprints. A network to provide such information could take years to create and cost up to $500 million; making it available to gun dealers could violate civil liberties. Beyond that, McCollum's system would not prevent gun sales to illegal aliens and the mentally ill.

"Still, a majority of House members reached for this fig leaf. They voted to kill the Brady amendment and replace it with McCollum's phantom plan. ..."

Just imagine what could go wrong if this legislation ever got past the Senate and the President, and such a system were implemented ...

Alan Kaminsky P.O. Box 9887
School of Computer Science Rochester, NY 14623
Rochester Institute of Technology 716-475-5255

Olympian RISKS

Henry Cox <cox@spock.ee.mcgill.ca>
Thu, 22 Sep 88 19:57:51 edt

ROOF RIPS AGAIN [From the Montreal Gazette, 9 Sept. 1988]

The Olympic Stadium's fabric roof suffered yet another rip yesterday - this one three meters long. [I have no idea how many other rips there have been.]

The Olympic Installations Board said in a statement it was disappointed by the mishap, which happened during tests of the roof's automatic retracting mechanism, because workers had got the roof-opening procedure down to below one hour. The board said computer controls on one winch weren't working, placing uneven tension on the fabric. Repairs should be done by tomorrow.

[Not a great story, but, after legendary cost over runs, an Olympic deficit that we are *still* paying off, and a roof that finally came 12 years late (and at approximately the cost of a *complete* covered stadium), I thought the Stadium roof deserved a mention in RISKS.]
Henry Cox

Sewage Spill Linked to Computer [BTW, See RISKS-7.7]

Nike Horton <horton%reed.uucp@RELAY.CS.NET>
Thu, 22 Sep 88 09:42:36 PDT

SPILL LINKED TO COMPUTER
The Oregonian (Portland, OR) Sept 22, 1988 page B2

A computer programming error combined with a burned-out wire led to a sewage spill into the Willamette River this week, said J. Michael Read, supervisor of the Tri City Service District. District technicians estimated Wednesday 1.5 million gallons of sewage spilled into the Willamette near the mouth of the Clackamas River late Monday and early Tuesday, Read said. The district serves about 40,000 persons in Oregon City, West Linn and part of Gladstone. The state Department of Environmental Quality lifted its warning to stay out of the river below Willamette Falls at 7am Wednesday.

While the burned-out wire stopped the sewage treatment pumps, he said, a programming error kept an automatic telephone dialing mechanism from signaling anyone that the machinery wasn't working, Read said.

District employees will be checking other alarms to see if any similar problems exist in the system, which is less than 2 years old, Read said. A

back-up alarm, which was being installed at the time of this week's spill, may be operating by the end of the week, the supervisor said.

[Readers may recall earlier sewage spills into the Willamette River, also blamed on the computer, and noted in RISKS-7.7 in a contribution from Randal L. Schwartz:

June 1988: "Sewage flows into river; computer failure blamed" -- The five-hour spill from the Sullivan Pump Station poured about 5.4 million gallons into the Willamette River downtown.

June 1985: Another computer failure caused the dumping of more than 3 million gallons of raw sewage into the Willamette from the same pump station.

Perhaps that is a new meaning for "garbage in, garbage out." PGN]

Keep backups, risk job

<jimc@math.ucla.edu>
Fri, 23 Sep 88 09:07:48 PDT

From Los Angeles Times, 9/23/88, page 1 (Mark Gladstone and Paul Jacobs, Times Staff Writers):

"The day after the FBI raided [state] Capitol offices last month, a legislative employee noticed a tenfold increase in the purging of documents from the legislative computer system and acted quickly to save the material ... Paul Hueslkamp, who works in the legislative data center, confirmed that he and co-worker Michael E. Parr were suspended by the legislative counsel's office pending the outcome of an internal investigation.

"Parr, a 15-year state employee and a data processing supervisor, refused an order by his superiors to erase the computer tapes, feeling it would be construed as an obstruction of justice, Huelskamp told The Times. ...

"Instead of the typical 70 to 80 computer deletions, Huelskamp discovered 750 to 800. The employee quickly extended the life of backup tapes until the end of the year. Normally, they would have been automatically erased after 14 days. 'I thought it might be useful for the FBI,' said Huelskamp ...

"The GOP sources said that the caucus staffers, aware it is illegal to conduct political campaigns with public resources, were worried that FBI agents would discover the material in the state computer. ...

"The legislative counsel, according to the source, ordered the internal investigation because he felt the traditional lawyer-client relationship may have been violated by the employees. The legislative counsel is the lawyer for the legislature and also controls the computer system."

[Disclaimer: Opinions herein are mine and are not to be construed as representing those of The Regents of the University of California.]

James F. Carter (213) 825-2897
UCLA-Mathnet; 6608B MSA; 405 Hilgard Ave.; Los Angeles, CA 90024-1555

Computer failure shuts down several thousand telephones

Vince Manis <manis@grads.cs.ubc.ca>
Thu, 22 Sep 88 11:38:52 PDT

According to a story in yesterday's Vancouver Sun, a failure at a telephone switching centre caused several thousand phones in an area on the west side of Vancouver to be inoperative for about 1 hour. Apparently, the phones would accept incoming calls (and ring), but would not permit outgoing calls to be made (including, one assumes, 911 calls). There was no report of any personal injury or loss as a result of the outage.

A BC Telephone Co. spokesperson said that the failure was due to a `computer bug', but couldn't be more specific. The centre in question serves a number of exchanges, but only part of one exchange was affected.

Vincent Manis, Department of Computer Science, University of British Columbia
Vancouver, BC, Canada V6T 1W5 manis@cs.ubc.ca

LA Times photo of humorous credit card maybe not so funny

Michael Coleman <coleman@CS.UCLA.EDU>
Thu, 22 Sep 88 12:49:35 PDT

(Reproduced without permission from the Los Angeles Times, 9/22/88)

Citibank Visa Gives Credit Where Credit Isn't Due
by Douglas Frantz, Times Staff Writer

Doris A. Stokes applied for a Visa credit card from Citibank over the telephone a few weeks ago. When a Citibank employee asked Stokes if she wanted a second card for another family member, she replied, "Maybe later." Her shiny new Citibank Visa card arrived at Stokes' Los Angeles home this week. So did one for Maube Later. "I brought it down to work, and everybody here was in tears laughing so hard about it," said Stokes, and administrative assistant at the Los Angeles Junior Chamber of Commerce. The response was more subdued at the New York headquarters of Citibank, the nation's largest bank and the world's biggest issuer of Visa and MasterCard credit cards. "Are you serious?" asked Susan Weeks, a bank spokeswoman in New York, when the incident was described to her. Assured that the talk was true, she groaned, "Oh, no." (rest deleted)

(Appearing above the article is a large picture of a smiling Doris A. Stokes holding a Citibank Visa with the name Maube Later.)

While the story itself is somewhat amusing, I wonder more about the wisdom of using that particular picture. In it we can clearly see everything on the card, including the number (xxx8 140 851 226), except for the first three

digits, which are obscured by Stokes' finger. This apparently is to keep someone from using this information for illegal ends. But wait, if Citibank is "the world's biggest issuer of Visa ... cards", perhaps I have one laying around. Here it is: the bank number (the first four digits) is 4128. Oops.

Risks of Cellular Phones?

Chuck Weinstock <weinstoc@SEI.CMU.EDU>
Mon, 19 Sep 88 10:14:00 EDT

While discussing radio triangulation last night, the question came up: If I dial a phone number attached to a cellular phone, how does the cellular system know which cell should send the ring signal to the phone? Is it a system wide broadcast, or does the cellular phone periodically broadcast a "here I am" signal?

If the latter, a less than benevolent government (or phone company for that matter) could use that information to track its citizens' cars' whereabouts. In an industrial setting, a competitor with access to the right information could track a sales reps sales calls to develop a client list.

Chuck Weinstock

Auto Computer Risks

Chuck Weinstock <weinstoc@SEI.CMU.EDU>
Mon, 19 Sep 88 10:09:06 EDT

On occasional Sundays I participate in time-speed-distance (TSD) road rallies. The object is to follow a course (on public streets) driving it at exactly the right speed as given by the instructions. Your car is timed as it passes certain points not known to you in advance, and you are assessed a penalty for every 1/100th of a minute you are early or late. The person who creates the rally tries to write the instructions so that they are accurate but mistake prone, so course following can be tricky.

To avoid the constant need for on-time calculations (to free up time for the navigator to help stay on course), many experienced rallyists run with special purpose digital computers hooked up to record distance and display timing information. These are hooked into the car's electrical system for power.

A friend just purchased a new Ford Probe (Mazda) and the service manager told him to be careful how he wired anything into the electrical system as the car had its own computer on board. My friend decided one day to try his rally computer out and used a cigarette lighter adapter to hook up the power. The computer seemed to run ok, but when he later started the car, it would not idle. It would start fine, and he could drive it as long as he didn't take his foot of the gas. If he did the RPM's would drop to zero and the car would stall. He removed his computer and drove the car for about 10 minutes and things got back to normal. He has subsequenty wired his computer into the

electrical system directly and has had no further problems.

One wonders if a radar detector or a cb radio (two common appliances that use the cigarette lighter) would cause the same difficulty.

Chuck Weinstock

Volvo's and Electromagnetic Interference

"BILL WELCH, BCD COMPUTING CENTER, (614)424-7155" <WELCH@battelle.arpa>
Mon, 19 Sep 88 15:22 EST

I own two Volvos - a 1984 and a 1988 DL245 station wagon. Both cars suffer strange effects to various computer/electronic systems in the present of radio signals. When I use my HAM radio transmitter on the 2 meter FM band (144..148 MHz) both have problems. The 1984 cruise control drops out, and on the 1988 the turn signals blink twice as fast as normal and the speedometer drops to zero.

> [We have had a bunch of messages on this subject in past issues, but the problem has evidently not gone away. PGN]

Scientific Safety

B.Littlewood <sd396@CITY.AC.UK>
22 Sep 1988 15:43:24-WET DST

I'm sorry William Murray has problems with my English. In the case of the Airbus A320 the notion of an "acceptable level of safety" is, unusually, spelled out by the manufacturers of the critical fly-by-wire system. They say that the reliability REQUIREMENT is 10**-9 failures per hour (see paper by Rouquet and Traverse in Proceedings of SAFECOMP 86). Their reason for adopting such a demending requirement is that (in their own words) " . . loss of . . function cannot be tolerated."

In a case like this it would, I think, be perverse to regard the system as "acceptably safe" if it had not satisfied the manufacturer's own requirements. Let us be charitable and take it that this requirement is not merely necessary but but sufficient for the award of the coveted status of "acceptably safe".

My assertion was simply that, in these terms, the A320 had NOT been demonstrated to be "acceptably safe". Indeed I believe that such cannot be demonstrated. I would go further and offer an opinion that the actual achieved reliability of the system is orders of magnitude less than this requirement.

Murray goes on to say that such novel technology would not be tolerated in the US unless it could be "proved" to be safer than the technology in use. This seems to me a pretty acceptable way forward, and I assume that it would not require demonstration of the achievement of ludicrous figures such as that above. However, even this more modest goal has not been demonstrated and it is my understanding that it will not be required before the plane gets a US certificate. Given the role played by software in this system,

and the absence of a fully functioning mechanical back-up, I do not believe that such a demonstration is possible.

I have a lot of sympathy with Murray's comments on our blithe acceptance of the mayhem which results from automobiles, tobacco, etc., and the difficulty of getting this on the political agenda. It would be a pity, though, if manufacturers of aircraft were allowed to get away with building less safe systems than hitherto, merely by appealing to the fact that flying is safer than smoking!

Bev Littlewood, Centre for Software Reliability, City University London EC1V 0HB

Computer Defaults (was: The Mental Tyrrany of Cash Registers)

Stephen Rickaby <sfr@praxis.UUCP>
Wed, 21 Sep 88 14:52:10 BST

Reading comments in RISKS about implicit belief in computers reminded me of a phenomenon I encountered in a previous job. Faced with the task of producing a large volume of related software, one of the tasks we undertook was the design of a common i/o library, partly for efficiency and partly to ensure a uniform `feel' across the software.

As our terminals were pretty much glass teletype mode, one attempt to introduce an element of user-friendliness was to give as many interactive screen routines as possible 'hot defaults': a suitable value for the parameter being requested would be displayed in braces ([thus]), this convention (HP and others) meaning 'the value you will get if you press <return>'. The slight touch of sophistication was that (valid) alternative values entered were swapped into the [braces], and <return> alone was required to confirm them. The system worked quite well, particularly for largely numerical interfaces for programs with a large iterative content and small changes in parameters for each iteration, typical of mathematical modelling and similar applications.

However, much of this software was for computer-assisted ATE work, performed by staff who had a very sound grasp of the work they were doing but not necessarily of computers. After a while, the following phenomenon was noted: when the default parameters were presented, they were often accepted even though the operator did not know a suitable value or even *thought they were wrong*. This was not out of laziness or a reluctance to use a keyboard, but because *the computer had suggested a value*, so it must be correct.

We never solved this one, and I left before the megawatt RF amplifiers were automated...

Steve Rickaby, Praxis Systems plc, 20 Manvers Street, Bath, BA1 1PX, UK,
Tel: +44 225 444700 sfr%praxis.uuc@ukc.ac.uk !mcvax!ukc!praxis!sfr

---

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 58

Monday 26 September 1988

Contents

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

Computers in local govt - a burning issue?

Dave Horsfall <dave@stcns3.stc.oz.au>
Fri, 23 Sep 88 09:47:42 est

Just read in the daily paper that a mayor ordered the air-conditioning in a computer room to be turned off, as the noise was interfering with the council meeting. Unfortunately, no-one ordered it turned on again, and the staff turned up next morning to find one cooked computer...

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

---

North Cornwall water supply polluted

Willie Smith, LTN Components Eng. <w_smith%wookie.DEC@decwrl.dec.com>
26 Sep 88 14:11

A combination of circumstances at an unattended water-works caused the pollution of the water-supply to 22,000 homes in north Cornwall by aluminium sulphate last July.

The following scenario was given by a TV programme last week. A relief driver was asked to deliver 20 tons of aluminium sulphate to an unattended waterworks. He was given a key to open the gate by the normal driver. This key should not have been available to the driver. The tank to store the aluminium sulphate was unlabeled, and the driver dumped his load into an underground reservoir of treated water. This water entered the water distribution system, now containing a amount of aluminium 500 times the maximum permitted. The water was now acidic (sulphuric acid), and started dissolving lead and copper from the pipes.

When notified of a problem, the water board discovered a mal-functioning pump. They repaired this and dumped the contents of the reservoir into the river, poisoning thousands of fish and other river life. They stated the water was now safe to drink. (It wasn't!!). Many animals died, and humans suffered much pain and discomfort. The long term affects of the pollution are unknown.

What has this to do with computing RISKS? The waterworks was automated, but all measuring devices were on the intake side of the waterworks. Designers had omitted to monitor the water exiting the works and entering the public supply, thus ensuring that the above sequence of errors was not picked up until the water reached the consumers!

BTW, under British Law, no crime has been committed.

Re: Risks of cellular telephones [RISKS 7.57]

<ark%hoder@CS.RIT.EDU>
Mon, 26 Sep 88 10:25:53 EDT

Chuck Weinstock asks how an incoming call is placed to a cellular telephone, and whether Big Brother could somehow use this to monitor persons' whereabouts. I used to work on cellular telephone switching system software, so I'll take a stab at it.

When a call is placed to a cellular telephone, a "paging" message is broadcast in all the cells in the system. Certain frequencies are set aside solely for paging. All active cellular telephones are constantly monitoring the paging channel. When a phone detects a paging message with its own address, it broadcasts a page response message. This response is received by all the cells in the system, and the signal strength is measured. The cell receiving the strongest response is assumed to be the cell in which the phone is located, an unused frequency in that cell is assigned, and the phone call is switched to a transceiver in that cell.

So cellular telephones are indeed located by a broadcast message, not by having the phones transmit periodic "here I am" messages. If no one is calling a particular cellular telephone, there is no way to know where that phone is. HOWEVER ...

While a cellular telephone call is in progress, the phone may move into a different cell. If it does, the call must be "handed off:" the connection must be switched from the transceiver in the current cell to an unused transceiver in the new cell, usually on a different frequency. The current transceiver constantly monitors the phone's signal strength; when it falls below a threshold, a handoff is needed. All the cells broadcast another paging message to the phone, the phone responds, the signal strengths are measured, and the cell receiving the strongest signal is the new cell.

Thus, _while_a_cellular_telephone_call_is_in_progress_ (either incoming or outgoing), the system knows the cell in which your phone is located, and unscrupulous parties could abuse this information. In between calls, you're safe.

As for business competitors monitoring calls you place on your cellular telephone, to find out your clients' phone numbers: This is perfectly possible. However, you'd have to get your hands on the radio equipment used in a cell's base station, plus its controlling software, and change the software to record information about calls being placed. This is probably beyond most business persons' capabilities. One hopes the FCC, police, etc. would prevent anyone from offering such a product commercially.

Alan Kaminsky, School of Computer Science, Rochester Institute of Technology,
P. O. Box 9887, Rochester, NY 14623 716-475-5255

Re: Risks of Cellular Phones? (RISKS-7.57)

John Gilmore <gnu@toad.com>
Sun, 25 Sep 88 17:04:09 PDT

> If I dial a phone number attached to a cellular phone, how does the
> cellular system know which cell should send the ring signal to the phone?

The standard for communication between a cellular telephone and a base station is EIA Interim Standard IS-3-C (June 1986). I got my copy in Feb 1987 from Global Engineering Documents at +1 800 854 7179 or +1 714 261 1455.

At cellular phone power-up, the phone listens on a set of fixed frequencies for a control message ("overhead message") telling it which channels are locally used as paging channels. It then listens to all those channels, picks the one with the highest signal strength, and listens on that channel for overhead messages and "mobile control messages". One such control message is a "page", which indicates that the land system wishes to get in touch with a particular mobile (identified by its phone number). In a simple cellular system, this "page" would probably be sent by all cells; in a more complex system,

it could be initially sent in a likely cell or cells, and later
sent in all cells if no response was heard.

When a cellular phone receives a "page", it responds by transmitting
a "page response" on a "reverse control channel". This tells the land
system that the page has been received, and specifies which transmitter's
page it heard. That cell will respond with an "initial voice channel
designation" message, if it has a free voice channel. The phone responds
by transmitting an audio tone on that channel to indicate that it
has seized the channel. Then the land station sends an "alert" message
which causes the phone to ring its audible bell. If and when you answer
the phone, it turns off the audio tone and starts transmitting
your voice.

As you can see, it's possible for the cellular system to "page" your
phone and establish its whereabouts without ever sending an "alert",
which would let you know that your phone was active. In fact, there is
another order called "audit" which causes the phone to silently
transmit a message back to the system, without ever telling you. In
some cases it appears that the audit response includes the phone's serial
number as well as its phone number.

In normal operation a cellular phone will not transmit unless it is
paged or you ask it to make a call. There is no ongoing tracking of
idle phones, though specific phones could be targeted for tracking
by sending periodic "page" and "audit" messages to them.

If you want privacy I recommend not using a cellular phone. A possible
compromise would be to get a paging beeper and a cellular phone. Leave
the beeper on all the time and power off the phone. The beepers have
batteries that last for a month anyway, while the phone will die in
hours if on. When someone wants to talk with, they call your beeper and
punch in their number and/or a prearranged code. You receive the beep,
but your beeper does not transmit any response. If you choose to
respond, you can power on your phone, dial back to whoever beeped you,
talk, then power off the phone. You can only be traced for the duration
of the call (and, of course, the call is on the radio so it can be
overheard). I'm actually surprised that I haven't seen cellular phones
with built in beepers like this, since it extends your battery life.

If your cellular phone was modified to present itself to the system as a random
phone number and serial number (most conveniently obtained from recent traffic
heard over the air by the phone, since it isn't encrypted), you would not be
traceable at all -- nor would you be billed for the call. (Your phone's
transmission could be traced, but there is nothing to tie it to "you"). Making
calls that are charged to other people is against the law of course, but seems
to be common practice; there's an "underground" traffic in phones with this
kind of modified firmware.

Other voice mailbox risks reported

<Bahn@PCO-MULTICS.HBI.HONEYWELL.COM>

Sun, 25 Sep 88 12:39 MST

A local company specializing in hardware for the US Government has been cooperating with the FBI into an investigation of illegal use of their voice mail system. Recently when they hired a new employee when they wanted to set him up a voice mail box they discovered the password had been changed for the system administrator. Technical support from INTELLICOM (the manufacturer) determined that someone had created several new voice mailboxes and were using them for credit card data. Apparently the passwords had never been set when the VMB was received from the manufacturer. Intellicom has advised all their customers who use these systems to also disconnect their 800 service outside of hours as this serves to deter miscreants from inhabiting your VMB.

This appears to be a criminal twist on previous risks reported. Peter.

Auto Computers vs. radios

Steve Jay <shj@ultra.UUCP>
Sat, 24 Sep 88 19:42:59 PDT

In RISKS 7.57, Chuck Weinstock writes (regarding his friend's Ford Probe going nuts when a computer was plugged into the cigarette lighter):

> One wonders if a radar detector or a cb radio (two common appliances that use
> the cigarette lighter) would cause the same difficulty.

The owners manual for my 1988 Mazda 626 (mechanically the same as Ford Probe) has the following warning:

"If a mobile two-way radio system is installed improperly, or if a wrong type is used, the fuel injection system and the cruise control system may be affected. To avoid damage to your vehicle, be sure to check with an Authorized Mazda Dealer for proper installation of a mobile two-way radio."

The Shop Manual (the one they would sell me) contains an almost impossible to interpret diagram that attempts to show where NOT to run the antenna lead for a radio transmitter. There is no information about what "a wrong type" might be. I sure hope my Authorized Mazda Dealer has better information.

I wonder if the thousands of places that will install a CB radio for you are aware of the danger of doing it improperly in a Mazda. (I don't mean to pick just on on Mazda. I suspect the same is true for lots of cars.) Also, given that malfunction of the fuel injection system and/or cruise control could do damage to people, not just the vehicle, the warning should be a lot more prominent. I have no idea how the warning could be made available to whoever might own my car 15 years from now.

Maybe the Army should publish the locations of the radio transmitters that do in their helicopters, so I can avoid driving near them.

Steve Jay, Ultra Network Technologies, 101 Daggett Drive, San Jose, CA 95134

Internet: ultra!shj@ames.arc.nasa.gov uucp: ...ames!ultra!shj 408-922-0100

State Records via Computer

<Curtiss@DOCKMASTER.ARPA>
Sun, 18 Sep 88 15:12 EDT

From FLORIDA TODAY, Melbourne, Florida (a Gannett Company) without permission:

> TALLAHASSEE- For private investigators, the tools of the trade used to be trench coats, binoculars and soft shoes. But that was before the revolution. Now, private investigators are just as likely to be huddled over computer screens as they are to be hanging out in the bushes.
>
> Like a growing number of states, Florida last month set up a computer link that makes driver license and vehicle registration records available to anyone with a computer. To access corporate records, it costs $25 an hour, not including membership fees to Compuserve, which runs the system. For highway department records, it costs $60 an hour, and users have to deposit money in advance. Last year the state made about $80,000 from fees on the service.
>
> [Quotes from users]
>
> State officals say they're banking on the adage that time is money. The potential of saving time, and therefore tax money, is one of the reasons they expanded the program.
>
> The program was started in 1986 after the Division of Corporate Records did a study that showed the agency was only responding to 15 percent of the requests for corporate information, said David Mann, director of the division. "It was a way to get heavy users off the system," he said of the computer link. "It worked like a charm, and it didn't cost the state any money."
>
> Since installing the computer link, about 13,000 of the 70,000 requests the agency gets each day are being handled by the computer. And its response rate is now about 45 percent, he said.
>
> [more quotes from users]
>
> With the push of a button, a law firm can tell a client whether a corporate name he wants to use is already in use, whether a corporation interested in buying a piece of property may be on shaky financial ground and who the corporate officers are.
>
> Mann and David Jacobson, of the motor vehicles agency, said hundreds of firms from Seattle, Wash., to New York City have signed up for the service. The firms include insurance companies, banks, labor unions and law firms. But the prime users appear to be private investigators. Both Mann and Jacobson agree that it's likely the system will be expanded as it proves its usefulness. Mann and Jacobson also said steps have been taken to avoid state records tampering.

Part of the drive behind allowing computer access to state records is Florida's "Sunshine Law". A previous article said that only the information listed on your driver's license and vehicle registration will be available. This information is ruled to be information of public record. Driving infraction histories will not be accessable.

William Curtiss

Damage by Disney 3-D glasses

Mon, 19 Sep 88 13:24:34 PDT

> "Please do not take these glasses as a souvenir.
> They will impair your vision outside this theatre."

The sentence is literally true. The glasses are not completely transparent; they absorb a small fraction of the light passing through, and so one's vision, while wearing the glasses, is impaired.

Until reading this posting, I never considered the more sinister interpretation, that one's vision would be permanently impaired.

-=- Andrew Klossner (decvax!tektronix!tekecs!andrew) [UUCP]
(andrew%tekecs.tek.com@relay.cs.net) [ARPA]

[Also noted by "Robert J. Reschly Jr." <reschly@BRL.MIL>
linden@Sun.COM (Peter van der Linden)
seanf@ucscc.UCSC.EDU (Sean Fagan)
jurjen@cwi.nl (Jurjen N.E. Bos, CWI, Amsterdam)
roskos@ida.org (Eric Roskos)]

re: more on killer remote controlls

GREENY <MISS026@ECNCDC.BITNET>
Mon 19 Sep 1988 16:09 CDT

> Caution: Use of this remote on another TV set could damage it...(or something
> along those lines....)

I find it *VERY* hard to believe that anyone would believe this claim by a hotel. This is simply a way to keep moronic, paranoid people who want to be a cleptomaniac for a day from stealing the remote control (as if it would actually work on their TV set at home...:->)

To date, I have about 10 IR controls in and about my house and I have found only two of them that have signals close enough to cause problems (they are easily worked around...but still). And I find it even harder to believe that an IR control could be engineered to "figure out" what type of signal was sent to your TV to turn it on/off, and to do so at such a pulse rate as to cause your TV to die....nope, just cant believe it. Maybe it could be done if they knew what kind of TV you had at home, but why? Basically, if the hotel in question had any brains at all, they would simply install a proximity type detector and put one of those little metal strips inside of the control. Then when you left your room, an alarm would sound. And to further reduce costs, ONE detector could be installed at the bottom of the stairs or other heavily used guest exit point....

..I guess this is just one more example of how gullible the public really is...
Greeny

Bitnet: MISS026@ECNCDC

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 59

Thursday 29 September 1988

Contents

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

Arthur Miller, Assault on Privacy: Computers, Data Banks and Dossiers

"Barry C. Nelson" <bnelson@ccb.bbn.com>
Wed, 28 Sep 88 11:03:40 EDT

The American Society for Industrial Security is holding its annual seminar and exhibition in Boston at the moment. There were nearly 3000 registered attendees, not including over 350 companies with product or service exhibits.

The luncheon speech on 27 Sept was by Arthur Miller, Professor of Law at Harvard University, renowned author on court procedures and legal expert appearing on TV programs such as "Good Morning America." He is author of "The Assault on Privacy: Computers, Data Banks and Dossiers" which is considered "must" reading on the issue.

Let me pass on a few of his remarks which were addressed to the thousands of security professionals from all over the country. It was shrill, but compelling. (Consider that MOST of the listeners know nothing about computers.)

Barry C. Nelson

++++++++++++++++ The following is provided without permission and may be available on tape from National Audio-Visual Transcripts, Ltd. ++++++++++++

"...
I warn you, I'm a card-carrying privacy nut.
...
You can't get very far in this world without your dossier being there first.

Flight Reservation systems decide whether or not you exist. If your information isn't in their database, then you simply don't get to go anywhere
...
What people have been reduced to are mere 3-D representations of their own data.

The Avis WIZARD decides if you get to drive a car. Your head won't touch the pillow of a Sheraton unless their computer says it's okay.
...
This information forms a permanent "dossier". It's THEIR information now.

They know your name, address, telephone number, credit card numbers, who ELSE is driving the car "for insurance", ... your driver's license number. In the state of Massachusetts, this is the same number as that used for Social Security, unless you object to such use. In THAT case, you are ASSIGNED a number and you reside forever more on the list of "weird people who don't give out their Social Security Number in Massachusetts."
...
YOU can't get a copy of these records. There is no law which forces private agencies to tell YOU what they know in most cases.
...
Data is a lot like humans. It is born. Matures. Gets married to other data, divorced. Gets old. One thing that it doesn't do is die. It has to be killed.
...
At the same time, data is dehumanizing. Take the case of a person, flesh and blood, who wants to go to law school. A six-page form is filled out and gets "processed" by the computer along with transcripts and LSAT scores. ...

Eventually an "index number" is spit out. This number is then put on the Great Chart on the Wall with a lot of others.

This person, whose only crime in life was wanting to go to law school, has been reduced to a DOT on the wall awaiting evaluation.
...
What should we be doing about all of this? Adjusting the regulations a little.
...
Only the information which is necessary for the job at hand should be collected.

People should have access to the data which you have about them. There should be a process for them to challenge any inaccuracies.

There should be more control on the eventual uses of data which was supplied for some business at hand, but has been sent elsewhere "upon request"

Old data should be killed when its useful life is served.

Data must be protected from those who would abuse it. ..."

EPROM is not necessarily programmed for life

<linnig@skvax1.csc.ti.com>
Wed, 28 Sep 88 09:23:18 CDT

Unless things have changed in the past few years...

UV erasable EPROM's only stay programmed for a few years (~7). These chips bury a charge inside of an insulating layer. UV exposure causes the charge to be erased, so does the passage of time.

I wonder how many computerized boxes out there are carry their programs in EPROM? Sounds like a ticking time bomb to me.

Mike Linnig, Texas Instruments

The Wobbly Goblin (a.k.a. Stealth fighter)

<ark%hoder@CS.RIT.EDU>
Wed, 28 Sep 88 07:20:32 EDT

"How Wobbly the Goblin" (Time magazine, October 3, 1988, p. 29)

"The U.S. Air Force is so secretive about its radar-invisible Stealth fighter that it refused to acknowledge the plane existed even when one crashed in California two years ago. Yet when a covey of U.S.A.F. pilots converged in Washington last week for an Air Force Association symposium, shop talk indicated that the Stealth has a nickname. Pilots who fly the plane out of the Tonopah, Nev., Air Force base find it so tricky they call it the "Wobbly Goblin." Onboard computers are supposed to control the Stealth's performance, even at the highest speeds, but experts say the plane sometimes "gets away" from the pilot, who then has to take over manually--and earn his wings all over again."

Does anyone know any details?

Alan Kaminsky, School of Computer Science, P.O. Box 9887, Rochester, NY 14623
Rochester Institute of Technology 716-475-5255

Re: Stanford Collider Shut Down <RISKS DIGEST 7.51>

Matthew P Wiener <weemba@garnet.Berkeley.EDU>
Sat, 24 Sep 88 23:57:36 pdt

>Stanford University's $115 million linear collider has been shut down
>after several months' efforts failed to get it running properly.

Is this *permanent*? I read only a month ago in SCIENCE (or NATURE?)

that they were still expecting to get results next year.

SLAC itself is not in trouble so much as the redesign for making it a
Z factory. Of course, there could be repercussions.

>Although there seems to be nothing basically wrong with the system, it
>is "simply so complicated that, despite the best efforts of more than
>100 people, they have not been able to keep all its complex parts
>working together long enough to get results."

Also, because they were in a hurry to beat CERN with the first Z factory,
they used the cheapest parts they could find. They are paying for this now.

One good consequence is that SLAC has proven that the basic design for
using linacs to mass produce Zs is sound. Nothing like it had been
tried before. I vaguely recall reading somewhere that inspired by
SLAC's "success", in West Germany there are plans to build a similar
linac-based Z factory.

>   Since spring they have
>"fought a succession of glitches and breakdowns in the machine's myriad
>magnets, computer controls, and focusing devices."

The outside weather did not help either.

ucbvax!garnet!weemba   Matthew P Wiener/Brahms Gang/Berkeley CA 94720

Re: Is Uncle Sam selling your name to mailing lists?

Mark Brader <msb@sq.sq.com>
Thu, 22 Sep 88 10:37:55 EDT

Path: sq!geac!yunexus!utzoo!utgpu!water!watmath!clyde!att!osu-cis!tut.[]
  cis.ohio-state.edu!mailrus!ames!necntc!dandelion!ulowell!interlan!pflaum
From: pflaum@interlan.UUCP (Greg Pflaum)
Newsgroups: misc.consumers
Date: 19 Sep 88 23:05:24 GMT
Organization: MICOM-Interlan, Boxborough, MA (1-800-LAN-TALK)

In article <2123@edsews.EDS.COM> peter@edsews.EDS.COM (Peter Zadrozny) writes:
>For the last two weeks I've been swamped with pre-approved
>credit cards and loans, at least three offers every day from
>different banks. The strange part is the they are all addressed
>to my legal name which is only known by Uncle Sam and his red tape
>offices. Is anyone of them selling names and addresses
>to mailing lists houses??? What's going on, are they going
>to pay the public debt this way?

It is possible that, at some point in the distribution, someone illegally
obtained a tape of names, addresses and other information from some
government database.

I've seen a similar situation when I was in school at the University of Massachusetts. I received a mailing from a life insurance company which was addressed to "The parents of Greg Pflaum". Because UMass did not have my parents' address, I often got mail from the school with that address. Checking around, I found that those friends who also received UMass's "To the parents of" mail had also received the insurance solicitation. I didn't check with any parents, but clearly at least some group of parents also got it.

At the office that produces the university magazine (Contact) that is sent to all parents I learned that mailing labels were ordered from a central office which did the database selection and printing. That was as far as I got. They said the school did not sell mailing lists, and refused to believe there was any connection between the insurance mailing and the UMass database. "Maybe someone went through the phone book," they suggested. Sheesh.

A student who did programming for the school suggested the most likely answer: a programmer or operator made a few bucks on the side.

Greg

CPSR 1988 Annual Meeting

Gary Chapman <chapman@csli.Stanford.EDU>
Sat, 24 Sep 88 14:07:06 PDT

Computer Professionals for Social Responsibility
Annual Meeting
November 19 and 20 at Stanford University

A collection of nationally known authors, scientists, and innovators in the computer science field will address the issues of computers and their impact on the arms race, the workplace, education, and society at the l988 Annual Meeting of Computer Professionals for Social Responsibility (CPSR), to be held November 19 and 20, l988, in Cubberley Auditorium at Stanford University.

Two sessions that already are generating a great deal of interest will draw together experts from a wide variety of fields to comment on developments in technology that could affect the general population.

The first, Privacy, Computers, and the Law, deals with the FBI's plans to upgrade its already massive criminal justice database so that it can better identify individuals. The current system now contains over l9 million records and is accessed up to half a million times per day. Would an improved version threaten the privacy and liberties of citizens? Discussing the issues from a variety of perspectives will be: William A. Bayse, FBI assistant director for technical services; Congressman Don Edwards (D-San Jose), chairman of the House Subcommittee on Civil and Constitutional Rights; Jerry Berman, chief legislative counsel of the American Civil Liberties Union and director of the ACLU Privacy and Technology Project; and Peter Neumann, SRI International and CPSR/Palo Alto.

The second panel will debate the impact of the personal computer of the future as presented in Apple Computer's video story, "Knowledge Navigator." The speculative Knowledge Navigator is a flat, notebook-sized computer that can speak with the user, explore databases on its own, do simulations, and display a picturephone and graphics, all by voice command. Addressing the social assumptions and implications of this possible technology will be: Larry Tesler, vice president of Advanced Technology, Apple Computer; Esther Dyson, editor and publisher of Release 1.0 newsletter; Fernando Flores, chairman of Action Technologies and co-author of Understanding Computers and Cognition; Peter Lyman, director of educational computing, University of Southern California; Theodore Roszak, professor of sociology, California State University at Hayward and author of The Cult of Information.

Speaking on the topic Technical Challenges in Arms Control in the Next 15 Years is Sidney Drell. Dr. Drell serves as co-director of the Stanford Center for International Security and Arms Control and deputy director of the Stanford Linear Accelerator Center. He also is past president of the American Physical Society and author of Facing the Threat of Nuclear Weapons.

Technology, Work, and Authority in the Information Age: The Role of the Computer Professional will address the opportunities and problems of computers in the workplace. By the end of the century, approximately two-thirds of all workers will use a computer terminal . Will that computer enhance their skills or assist management in controlling workers? Speaker Robert Howard, author of the book Brave New Workplace and senior editor of Technology Review will focus on what role computer designers can do to create socially responsible products.

Women learn how to use computers differently than men, says speaker Deborah Brecher, founder and executive director of the Women's Computer Literacy Program in San Francisco. Women and Computers: Does Gender Matter? will cover what programmers, educators and employers need to know about computer learning and the sexes.

Computer pioneer Jim Warren will deliver the keynote speech at CPSR's Annual Banquet to be held at Ming's Villa in Palo Alto. Mr. Warren founded The Intelligent Machines Journal which .later became InfoWorld. He also started the West Coast Computer Faire, the pre-eminent show for personal computer users and hobbyists, was the founding director of the first personal computer software magazine, Dr. Dobb's Journal of Computer Calisthenics and Orthodontia. He later served as the original host of the PBS series, "Computer Chronicles," and was awarded the first Sybex Computer Pioneer Award which recognizes innovators in the microcomputer field. In the academic arena, Mr. Warren has taught computer science at San Francisco State, San Jose State and Stanford University. Mr. Warren's speech, Computers, Information, and Politics, will focus on how citizens can gain access to computerized information on individuals, corporations, and the government, and how they can use that information to bring about effective political action, locally or globally.

During the banquet, the CPSR Board of Directors will present the Norbert Wiener Award for Professional and Social Responsibility to Joseph Weizenbaum, professor of computer science (emeritus) at the Massachusetts Institute of Technology.

Sessions on Sunday, November 20, will be devoted to the organization and future direction of the association. Speakers include: Terry Winograd, associate professor of computer science at Stanford University and co-author of Understanding Computers and Cognition,; grassroots organizer and trainer John Spearman, senior contract administrator for The Doctor's Council in New York City; Steve Zilles, chairman of the board of directors, CPSR; and Gary Chapman, executive director of CPSR and co-editor of Computers in Battle.

Registration fees for the meeting are as follows: $10/members; $20/nonmembers before November 9; $20/members, $30/nonmembers after November 9. The banquet is $30/members, $35/nonmembers. Reservations are on a first-come, first-served basis. Please call (415) 322-3778 for registration material.

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 60

Monday 1 October 1988

Contents

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

Diving Computers

Brian Randell <Brian.Randell@newcastle.ac.uk>
Sun, 2 Oct 88 13:42:13 +0100

Though there has I recall been discussion in RISKS before about diving computers, I have not before seen any publicity about problems in the UK. Here is an article from the Sunday Times for 2 October 1988, reprinted in its entirety, without permission.

Brian Randell

[See RISKS-6.51, 53, 55, 57, 59, 60, 63 for previous discussion! PGN]

DIVERS BLAME WRIST COMPUTER FOR `BENDS'
by Richard Ellis

Officials of Britain's biggest sub-acqua club are promoting computers for divers that some experts have condemned as potentially dangerous, and which could lead to divers getting compression sickness, or "the bends".

Two senior officials, including the chairman, of the 35,000 strong British Sub-Acqua club have financial links with a company that distributes one brand of the computers in Britain. Diving computers have been branded as potentially unsafe by Royal Navy diving experts, who say that they may be contributing to a rise in the number of divers suffering from the bends.

Sub-acqua club officials have been advised of the navy's concern, and of the worries of one branch where two divers using computers suffered the beds, but the officials have continued to advise members that the computers are safe, without declaring their financial interests.

The wrist-strap computers are designed to tell divers how long they can stay underwater and indicate how long they need to stop while ascending to avoid the bends. The traditional method is for divers to use a printed table supplied by the club.

The Institute for Naval Medecine, in Gosport, Hampshire, says that the cases of decompression sickness it has dealt with have doubled in the past year, during which time computers have become popular in Britain.

It says the computer software may be based on unsafe data, that it does not take into account such factors as age, fitness, sex and exertion, and therefore gives divers a false sense of security. Doctors at the institute last week called for extensive safety trials.

Surgeon Captain Ramsay Pearson, the institute's head of undersea medicine, said 34 of 80 cases of decompression sickness dealt with there this year involved the use of computers. "People are relying absolutely on the computers, and they are allowing people to do things we think to be unsafe," he said.

In August, the Brighton branch of the club wrote to senior club officials after two of its members needed treatment for the bends. Both had been wearing an Aladin dive computer, one of five brands available in Britain. The branch asked why no warning about the potential dangers of computers had been issued by the national headquarters.

The branch received a strongly worded six-page letter from Mike Holbrook, chairman of the club, dismissing the complaint as "mischief-making". He claimed there was no evidence of any problem with the Aladin, saying the data on which it was based was "tried and tested".

What the letter did not reveal is that Holbrook's full-time job is as a diving consultant for Spirotechnique (UK) Ltd, one of two importers and distributors of the Swiss-made Aladin computer in Britain.

The managing director of Spirotechnique (UK), a subsidiary of a French firm,

is Mike Busuttili, another leading member of the club, who is its former national diving officer and now a member of its decompression working party.

Around 5,000 of Britain's 50,000 divers now use computers. The Aladin, at a relatively cheap (pounds)199, has been one of the most popular brands.

Holbrook last week denied that there was anything improper about his twin roles. He said: "What's wrong? Can I not be objective? I think I can." He claimed club figures showed there had not been a rise in the number of divers getting the bends, and that investigations into cases of the bends where computers had been blamed had established other factors were responsible.

But Mickey Miller, chairman of the Brighton branch, said many of the 230 divers in his branch were worried, "Until this summer we had had just three cases of decompression sickness since we were formed in 1953. Now we have doubled that."

One of the three recent cases was Miller himself, though he was not using a computer. The two other Brighton men who got the bends - bubbles of gas that form in the blood and can cause paralysis or death - were using the Aladin.

They suffered slight numbness and recovered quickly. But a scan later showed two lesions on the brain of one of them, Peter van der Boon, a businessman. They have not affected his health.

Van der Boon, 37, a diver for 18 years, blames the computer for his attack. "It said I was in the clear, but it was not the case obviously. If there had been the slightest whisper from the national office about any problems, then I would not have got the bends. Now I only use the computer as a backup."

The Swiss firm Uwatec, which makes the Aladin, yesterday rejected allegations the gadget may be unsafe.

Ernst Voellm, the development engineer who helped produce Aladin, said 50,000 computers had been sold worldwide since 1983, and just a "handful" of cases of divers developing decompression sickness with them had come to their attention.

The Perils of PCs in Public

<Dave Horsfall <dave@stcns3.stc.oz.au<>
Fri, 30 Sep 88 12:08:23 est

From the "Rumour Central" column in PC Week, Sep 15:

``... On Thursday August 25, I was attempting to make a connection at Adelaide airport when a blackout occurred. Emergency lighting only, no PA system, no Arrivals and Departure screens, no seat allocation computer, and so on. When normality was finally restored, what should appear on the Australian Airlines monitor but a cute little picture of a hand holding a 3.5in disk with the familiar label 'Amiga KickStart'! Nobody did KickStart the thing for the next half-hour before I boarded the plane. For all I know, the passengers are still seeing this ghostly

hand instead of Arrivals and Departures. It seems that Australian
Airlines' mainframe is not up to the job of displaying a list of
Arrivals and Departures details in pretty colours.''

Although the intent of the article was about how PCs are being used in places where one expects to find a mainframe, I couldn't help but be amused by the RISKs present - no backup supply for the display computer, no auto-boot sequence, the possible harm to public relations when no-one realised the Amiga needed to be booted, etc.

Dave Horsfall (VK2KFU), Alcatel-STC Australia, dave@stcns3.stc.oz
dave%stcns3.stc.OZ.AU@uunet.UU.NET, ...munnari!stcns3.stc.OZ.AU!dave
PCs haven't changed computing history - merely repeated it

A New Portal for the Offensive -- FAX ATTACKS

Scott Rose <rose@cs.wisc.edu>
Fri, 30 Sep 88 20:15:05 -0500

Yesterday's Wall Street Journal had a hilarious (at least, at first...) front page article about the rapidly growing practice of sending advertisements to FAX machines. Besides being offensive, this technique is also reportedly very effective, because people tend to read their FAX traffic very carefully. So effective that an outfit in NYC is reported to be rewarding those who provide a list of 100 new FAX numbers with a new Sony Walkperson.

As personal FAX machines start becoming commonplace, there will surely be an epidemic of obscene transmissions. Unfortunately, a picture can be worth ten thousand words.

Is Uncle Sam selling your name? -- Maybe not.

Mark Brader <msb@sq.sq.com>
Sun, 2 Oct 88 14:53:02 EDT

I forwarded from misc.consumers to Risks 7.59 an article reading in part:

> > For the last two weeks I've been swamped with pre-approved credit cards
> > and loans, at least three offers every day from different banks. The
> > strange part is the they are all addressed to my legal name which is only
> > known by Uncle Sam and his red tape offices.

There have since been several follow-up postings recounting similar stories, and several followup posting pointing out that information "only known by Uncle Sam" is often a matter of public record if you know where to look. So while some data may be being distributed illicitly, in other cases, Freedom of Information laws are responsible for junk mail.

Mark Brader, SoftQuad Inc., Toronto, utzoo!sq!msb, msb@sq.com
The lawgiver, of all beings, most owes the law allegiance.
He of all men should behave as though the law compelled him.

> But it is the universal weakness of mankind that what we are
> given to administer we presently imagine we own. -- H.G. Wells

---

Re: Is UMASS selling your name to mailing lists?

Andrew Klossner <andrew%frip.gwd.tek.com@RELAY.CS.NET>
Mon, 3 Oct 88 12:19:10 PDT

[]

> "They said the school did not sell mailing lists, and refused
> to believe there was any connection between the insurance
> mailing and the UMass database. "Maybe someone went through
> the phone book," they suggested. Sheesh."

Sheesh yourself. My first summer job (as a teenager) was to do just that -- manually key the UCSB phone book into a junk mailing list.

-=- Andrew Klossner (decvax!tektronix!tekecs!andrew) [UUCP]
(andrew%tekecs.tek.com@relay.cs.net) [ARPA]
Organization: Tektronix, Wilsonville, Oregon

---

write your credit card number on a business reply card?

David Sherman <dave@lsuc.UUCP>
29 Sep 88 08:49:25 EDT (Thu)

The pre-registration card for the Canadian Computer Show, to be held in Toronto in November, invites you to send in the card with a cheque, or simply fill in your credit card number and expiry date and sign the card. It's got a business reply (no postage required) address on the back, so you just have to drop it in the mail.

Right.

The computer angle is that it's for the country's largest COMPUTER SHOW! These people should know better.

David Sherman, The Law Society of Upper Canada attcan!lsuc!dave@uunet.uu.net

---

Killer terminals

Mark Brader <msb@sq.sq.com>
Thu, 29 Sep 88 19:12:57 EDT

Michael Fischbein (msf@prandtl.nas.nasa.gov) writes: [in comp.misc]

> I worked designing microprocessor based fire and security
> alarm systems for skyscrapers, back when microprocessors were a
> brand new idea. Well, we had development systems from two

vendors and only one terminal. I came up with a cable to hook the ASR-33 up to the other development system so we didn't have to wait for that vendor to get a terminal to us. I carefully checked the connections, plugged the cable into the terminal and put a trusty VOM on the connections to make sure the signals were right.

OK. Both off, connect the ASR-33 to the computer. Turn on the computer. Turn on the teletype. POP! Hissss... Yank both cords out of the power strip. Notice blue smoke coming out of the computer. Go back and measure the signals on the data connector with an O-scope. Gee, there's a 40 volt AC square wave superimposed on the TTL signal.....

We tell the vendor of system 1 (that supplied the teletype) what's wrong with the teletype and ask for a replacement. No, that's the way it is supposed to work. Yep, sure it is. That's OK, they'll install it on their development system.

They plug the teletype to their machine when it arrives. POP! Hisss... They take it to their local distribution center, the service engineer checks it out thoroughly, ``repairs'' it, hooks it up to one of their systems. POP! Hisss.... Two systems later, he admits mystification and ships the killer teletype back to the factory in California. Last I heard, the teletype had vaporized three systems back at the factory and they couldn't figure out what was wrong.

mike

Michael Fischbein msf@prandtl.nas.nasa.gov
...!seismo!decuac!csmunix!icase!msf
These are my opinions and not necessarily official views of any organization.

Killer terminals

Mark Brader <msb@sq.sq.com>
Thu, 29 Sep 88 19:12:57 EDT

Bill Witts (william@cs.ucl.ac.uk) writes: [in comp.misc]

I used Televideo 910 terminals as an undergrad, and when you logged off, the system cleared your screen. Once, I typed LOGOFF and then realised I needed the data currently on the screen, so I hit CTRL-S hard just as the first carriage returns came through to scroll the screen. And the terminal just stopped - no logoff message, nothing - and nothing that I did made any difference. It was definitely the terminal that went, as I tried plugging different terminals into the same socket, and power-off didn't help. I couldn't believe this, so I replicated the situation and killed another terminal.

Later on, I mentioned this to a friend who didn't believe it either, so he promptly killed one and demoed it to someone else. Within an hour,

half of the college terminals were extinct which was amazingly popular
as it was the middle of the project season, and about a week later
the dead terminals were taken away and were replaced after a further week.

... Bill

Bill Witts, CS Dept. UCL, London, Errrp william@cs.ucl.ac.uk

This train didn't need a fireman

Chuck Weinstock <weinstoc@SEI.CMU.EDU>
Wed, 28 Sep 88 10:27:40 EDT

The following was found on the rec.railroad netnews. For background,
the Great Northern Railroad, now a part of the Burlington Northern,
has a long tunnel in northern Washington State (I forget how long, but
I seem to remember something like 8 miles.) In the days of steam
engines this presented a breathing problem so the railroad electrified
its operations through the tunnel, and would exchange electric
locomotives for steam at each end of the electrified district.

Chuck Weinstock

> From: earl@phred.UUCP (choo choo earl)
> Subject: Re: WHAT IF the Great Northern ?
> Keywords: anecdote
> Date: 28 Sep 88 00:38:39 GMT
> Reply-To: earl@phred.UUCP (choo choo earl)
> Summary:It's Electric
>
> My dad related a story about the Great Northern electrification. He said that
> the Forest Service had its central office for the fire lookout telephones
> in Skykomish, the change point to electric. It seems that the ringers in the
> phones were 20Hz, and the trains were 25Hz. When a train pulled out headed
> for the tunnel, ALL of the phones in all of the fire lookouts would ring
> continuously until the train was over the hump.
>
> Just something I thought people might like
> earl

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 61

Tuesday 4 October 1988

Contents

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

Program Verification: The very idea

Brian Randell <B.Randell@newcastle.ac.uk>
Wed, 5 Oct 88 9:56:39 WET DST

I have just finished reading, with great interest and enjoyment, an article by J.H. Fetzer with the above title, which appeared in Comm ACM 31,9 (Sept. 88) pp. 1048-1063.

In my opinion it is a very careful and lucid analysis of the dispute between, e.g., DeMillo, Lipton and Perlis on the one hand, and Hoare on the other, regarding the nature of programming and the significance of program verification. Its abstract is as follows:

> The notion of program verification appears to trade on an equivocation. Algorithms, as logical structures, are appropriate structures for deductive verification. Programs, as causal models of these structures, are not. The success of program verification as a generally applicable and completely reliable method of guaranteeing program performance is not even a theoretical possibility.

The final chapter, entitled "Complexity and Reliability", is the one which most explicitly relates to the interests of the RISKS readership but its understanding requires a careful reading of much of the earlier part of the paper. The final chapter, incidentally ends as follows:

> In maintaining that program verification cannot succeed as a generally applicable and completely reliable method for guaranteeing the performance of a program, DeMillo, Lipton and Perlis thus arrived at the right general conclusion for the wrong specific reasons. Still, we are indebted to them for their efforts to clarify a conclusion whose potential consequences - not only for the community of computer science, but for the human race - cannot be overstated and had best be understood.

Brian Randell

RISKS of EPROMS

Daniel Klein - 412/268-7791 <dvk@SEI.CMU.EDU>
Fri, 30 Sep 88 13:00:55 EDT

The UV eraseable EPROMS that are found in many smaller computers are also subject to failure when their picture is taken. Yep, you read that correctly. Once when I worked for the Computer Engineering Center, we were taking publicity photos of one of our process control systems. The system was working just fine, but as soon as we took the photo, it crashed. Surprisingly, the system right next to it did not. We rebooted, the processor, took another photo, and "blam", it crashed again. What was happening was as follows: the system that was crashing had the lid off, while the one running had the lid on. When we swapped the lid, the system that crashed changed also. We discovered that it was the flash that was causing the problems, and the either there ws enough UV being emitted from the flash, or simply that the light intensity was high enough to confuse the EPROMS for a few machine cycles, and cause bogus information to reach the CPU, crashing it.

Poor user interface -- police system

<rpg@CS.BROWN.EDU>
Mon, 3 Oct 88 21:07:09 EDT

Reprinted without permission from the Providence New Paper:

> Providence Police Chief Walter Clark was grilled on his department's position on police/minority relationships, the effects of drugs on the community, and the speed and attitude of officers responding to calls.

Answers and solutions were prompt.

Chief Clark explained that all calls to the police department are entered into a computer and prioritized, but only the 20 or so reports visible on the CRT can be acted on. Which is why it can take two hours for the police to respond to a burglary after the fact, as opposed to more immediate response to a burglary in progress.

It astounds me that the writers of such a piece of software wouldn't have provided for the display to scroll, especially considering that there are problems of starvation like this. And what happens if there is a disaster, like the New York blackout and widespread crime, such that there are more than 20 urgent calls to be managed?

Cash registers and tax

j eric townsend <erict%flatline@sri-unix.UUCP>
26 Sep 88 20:23:26 CDT (Mon)

During a break between classes the other day, I decided to restart my tradition of the "perfect student lunch": beer and grease. I got my usual: pizza, $1.50, and a domestic beer, $1.50. (Ouch, time to put the cooler back in the car... :-). I went to the register, and the button-pusher told me I owed $3.18. Normally, tax isn't charged on food at UH. What you see is how much it costs, EOL. I asked the clerk about this, as I'd gotten the same thing the day before, and it had only cost $3.

The clerk replied: "Oh, you probably got it at the other register. This is the only register that charges tax."

Me: "Well, give me back my $.18, then, since you don't normally charge tax."

Clerk: "Sorry, I can't do that, because the cash register says you owe $3.18."

There was a manager standing nearby who couldn't tell me if I owed tax or not...

Moral: If you eat in the Satellite at UH, don't go to the far left register, it charges 8 percent tax while the other registers don't.

(Actually, I think that UH adds the tax into the price of the food just to make it easier to figure out your bill. Then, the spend $$$'s trying to reverse-engineer their retail costs... :-)

J. Eric Townsend, 511 Parker #2, Houston, Tx, 77007
Inet: COSC3AF@george.uh.edu UUCP: uunet!nuchat!flatline!erict
Bitnet: COSC3AF@UHVAX1.BITNET ..!bellcore!tness1!/

Re: Cash registers

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

Thu, 29 Sep 88 14:29:39 PDT

We have previously had several tales such as the following, prompting someone to note that segmented number generators initially display an "8" in each position so that someone who is paying attention would notice when a segment is burned out. But in this case someone would have to use mirrors.

At lunch the scale for salads etc. has digital displays on two sides. I was on one side, the cashier on the other. She told me the amount -- $1.93. I noted that it said $1.83 on my side. She insisted that MY side had been wrong before that day and that they were using HER side. When told that the reason her side said "8" instead of "9" was that one of the segments was burned out, she finally acquiesced. But it occurred to me that a different segment had probably been out on my side, presumably in the units digit, which is what had prompted her to believe that HER SIDE was the right side. Groan. P.

Fly-by-wire, absence thereof

attcan!utzoo!henry@uunet.UU.NET <Henry Spencer>
Tue, 4 Oct 88 00:53:56 EDT

The hit of the Farnborough Air Show this year was definitely the MiG-29. The Soviets sent two of them, basically to show off. They did everything the F-18s and the like did, and a couple of things that nobody in the West had thought of doing with a jet fighter. The interesting thing is, unlike their Western competitors, the MiG-29s do not use fly-by-wire! They have plain old hydraulic controls, no computers involved. Doesn't seem to hurt flight performance, and the pilots claim the same "carefree handling" as the computerized fighters.

Henry Spencer at U of Toronto Zoology
uunet!attcan!utzoo!henry henry@zoo.toronto.edu

---

re: A New Portal For The Offensive -- FAX ATTACKS

GREENY <MISS026@ECNCDC.BITNET>
Tue 04 Oct 1988 17:46 CDT

Gee, I always thought that it was illegal to make use of the telephone to harrass, or say obscene things to people who didn't want to hear it (i.e. heavy breather sicko-types) -- or at least it is here in Illinois. And if I remember correctly, doesn't a receiving FAX print out the transmitting PHONE NUMBER somewhere on the transmission? If so, and you keep getting stuff that you don't appreciate -- just call the cops. If that doesn't fix the problem, try sending back what ya got! :->

Greeny

Re: Is Uncle Sam selling your name to mailing lists?

Matthew Huntbach <mmh@doc.imperial.ac.uk>

Tue, 4 Oct 88 20:11:31 BST

In the U.K. the electoral register is obtainable in most places in computer readable form. It is fairly easy to use it to target names in fact mailing companies have produced directories mapping postcodes onto average prosperity. Also the changing fashions for first names can enable a good guess at ages.

Clearly the electoral register has to be made available to candidates. As a political activist myself, I know the value of computers in fighting elections. But even if you only gave the register to candidates, what is to stop a mailing list company putting up a candidate simply to get hold of the register?

More on monitoring Cellular Phones

<linnig@skvax1.csc.ti.com>
Tue, 4 Oct 88 18:01:58 CDT

Alan Kaminsky (ark%hoder@CS.RIT.EDU) writes:

> When a phone detects a paging message with
> its own address, it broadcasts a page response message. This response is
> received by all the cells in the system, and the signal strength is measured.
> The cell receiving the strongest response is assumed to be the cell in which
> the phone is located, an unused frequency in that cell is assigned, and the
> phone call is switched to a transceiver in that cell.

Ah, but could the phone company send out a page without a following "ring them" message? If they could, then they could periodically poll your position, and your faithful cellular phone would report it without your knowledge.

> As for business competitors monitoring calls you place on your cellular
> telephone, to find out your clients' phone numbers: This is perfectly
> possible.... One hopes the FCC, police, etc.
> would prevent anyone from offering such a product commercially.

Well, the communication privacy act recently passed prevents you from intercepting the audio side of the cellular phone conversation, but I doubt if it prevents you from picking up the dialing info. I think such a device might be considered in the same class as a "pen register." Pen registers record the numbers called on a telephone circuit. I believe the Supreme Court doesn't even require a search warrant to place a pen register on a phone. It may be quite legal to record the phone numbers dialed by a cellular phone. Someone with a law background want to comment?

Mike Linnig,
Texas Instruments

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 62

Friday 7 October 1988

Contents

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

Re: Assault on Privacy (Arthur Miller's speech, via Barry C. Nelson)

"Anthony G. Atkielski" <Atkielski@PCO-MULTICS.HBI.HONEYWELL.COM>
Fri, 7 Oct 88 15:38 MST

Seriously, many of the concerns Mr. Miller voiced in his speech have already been addressed outside the United States. Specifically, France has had legislation regulating the establishment and operation of virtually all databases containing sensitive information about specific individuals for over ten years.

French Public Law 78-17 of January 6, 1978 established a Commission on Freedom and Computers and set forth requirements to be met by any organization wishing to collect and process "personal" information, i.e., information that can be linked to specific individuals. The Commission is a relatively autonomous organization charged with tracking the establishment and operation of databases

containing "personal" information throughout France. Its members are selected from both the public and private sector.

Some provisions of this legislation address certain of Mr. Miller's concerns specifically, for example:

> YOU can't get a copy of these records. There is no law which forces
> private agencies to tell YOU what they know in most cases.

In France, Public Law 78-17 requires that most organizations maintaining databases containing personal information declare the existence and purpose of these databases to the Commission on Freedom and Computers. These declarations are a matter of public record. These organizations MUST provide an individual with a copy of any information they may have on him (except for medical records, which must be requested through a licensed physician) on demand, and they must provide the name and location of an agent through whom such requests may be submitted in their declaration to the Commission.

> Data is a lot like humans. It is born. Matures. Gets married to other
> data, divorced. Gets old. One thing that it doesn't do is die. It has
> to be killed.

The French legislation requires that expiration periods for various classes of data be specified in the declaration to the Commission. The organization submitting the declaration must observe the expiration periods it declares.

> Only the information which is necessary for the job at hand should be
> collected.

Law 78-17 restricts the use of information concerning religious beliefs, lifestyles, political beliefs, race, union membership, and legal records (arrests, etc.) to organizations with a bona fide business interest in this information (e.g., political parties, churches, unions, police departments).

> People should have access to the data which you have about them. There
> should be a process for them to challenge any inaccuracies.

As already mentioned, this mecanism exists in France. An individual may force organizations to correct or update any information they may have on him. They are also obligated to correct and update information on their own initiative as they become aware of inaccuracies.

> There should be more control on the eventual uses of data which was
> supplied for some business at hand, but has been sent elsewhere "upon
> request"

Organizations must describe exactly with whom and under what conditions they will share the information they have gathered in their declarations to the Commission. They must also propagate corrections and updates to these third parties as they become necessary.

Public Law 78-17 requires that the following information be made available to the public for any organization collecting and processing personal data:

-- the identity of the organization
-- the types of data being collected, their sources, the periods of their retention, and the identities of any organizations or individuals to whom the data might be communicated
-- the purpose to which the collected data is to be put
-- the agent through whom an individual may exercise his "right of access" to data collected by this organization concerning himself
-- the categories of persons who might for any reason have direct access to the data
-- the relationships defined between the various data collected for a given individual
-- the types of security measures taken to ensure the confidentiality of the data
-- the manner in which the data are communicated to organizations or individuals outside France, if applicable

All individuals have the right to oppose the collection of personal data concerning themselves, except when such collection is required by government agencies. This implies that they may insist that, say, a credit bureau erase all information concerning themselves from its database.

When personal information is collected from a person, that person is entitled to the following information:

-- whether or not the information requested is required or optional
-- what will happen if they refuse to provide the information
-- the persons or organizations to which the information will be communicated
-- the fact that they are entitled to inspect and correct the information being collected ("right of access")

This part at least resembles the U.S. Privacy Act of 1974.

The French legislation also provides penalties for those who fail to heed the law. Organizations collecting data without filing a declaration may be subject to a $31,000 fine and a three-year prison term (the prison term would apply the individual(s) responsible for the violation). Collecting information forbidden by the law (religious affiliation, etc.) is punishable by a $310,000 fine and five years in jail. Revealing confidential information to unauthorized persons is punishable by a $3100 fine, plus six months in jail if the act was deliberate (as opposed to being the result of carelessness or negligence). Finally, a $310,000 fine and five years in prison awaits anyone who deliberately uses personal information for a purpose other than the purpose declared to the Commission.

As far as I know, no legislation in the U.S. even comes close to this; if there is any such legislation, it is being ignored. Maybe it's time we enacted something similar here in the U.S.

Anthony Atkielski, Honeywell Bull Inc., Phoenix, AZ, U.S.A.

Interesting article in PCW

<"hugh_davies.WGC1RX"@Xerox.COM>
7 Oct 88 03:54:25 PDT (Friday)

The current edition of Personal Computer World (October) has a long and interesting article on the application of the Data Protection Act, by Duncan Campbell. ('On and Off the Record', P146). I have no intention of keying the article in as it is several thousand words, but in essence it states that the application of the DPA is effectively being sidestepped by Government Departments, and that the Data Protection Registrar is toothless, underfunded and overwhelmed with pointless paperwork.

Campbell, who has been a thorn in the side of Government secrecy for some years, attempted to get a copy of his records on the PNC (Police National Computer). He was at first unable to locate a copy of the Data Protection Register, which lists all the registered computer systems in the UK. There is supposed to be a copy in every Public Library, but most had never heard of it. When he finally located a copy, the Librarian was reluctant to let him look at it. Once he had found out which systems the PNC have, he then couldn't find out who to write to. The DPR said write to the Data Protection Officer at the PNC, but no-one ever replied. Finally he tried several local police stations, but most denied knowing anything about it. Once a police station accepted the query, they gave him a form to fill in which asked several irrelevant and personal questions. Finally, he got a reply from the PNC, 40 days after putting in the query (the legal maximum time allowed). The DPA allows for a charge of #10 for each query on each system, he queried each of the 5 systems running at the PNC and was charged #50. He was refunded #10 because the PNC said that they could not be bothered to inspect one of the files, because "there won't be anything on it".

This whole shambles would appear to be mainly designed to deter anybody from attempting to use the DPA to enquire on Government (or indeed, any other) computer systems. Campbell conludes that the DPA is a complete failure, and after reading the article I agree with him.

Also, some more interesting information on the PNC has recently come to light. The British Government is busily (and fairly quietly) installing a system to connect all the computer systems belonging to such organisations as the Inland Revenue, Department of Health and Social Security and the Driver and Vehicle Licensing Centre. This system is called the Government Data Network, or GDN for short. Virtually no information has been forthcoming about this system. It has been denied that the Police National Computer is to be part of this network, but it has recently become clear that this is not the case. The reason being that the present PNC is indeed not to be connected to the GDN. However, the soon to be installed upgrade to the PNC, being imaginatively called 'PNC2' *IS* to be connected to the GDN.

Hugh Davies, Computer Consultant, St.Albans, England.

The opinions expressed herein are mine, not those of my current, or any past, employer or client.

Bridge over troubled pseudo-random generation

Peter Neumann <neumann@csl.sri.com>
Fri, 7 Oct 1988 14:42:30 PDT

Computers are now being used for all sorts of purposes for which people formerly did the same job. A case at hand deals with the game of bridge, in which shuffling for tournament matches is now done by computer. Alan Truscott's column in the Sunday New York Times (2 October 1988) relates that during the team-of-four matches the players sensed that the hands were strangely familiar. The American Chip player Martel "eventually solved the problem: All the deals corresponded to those most of the players had encountered in the open pairs final four days earlier, but with a suit rotation -- spades had become hearts, hearts diamonds and so on. The computer program that generated the deals for both events was suffering from a flaw in its random generator." (The bridge rules state that a deal previously played must be null and void. Apparently that rule was extended on the spot to include suit transformations.)

> [Thanks to Paul Abrahams for this one. Now that he is no longer President of the ACM, I presume he has a little more spare time to keep an eye out for us on computer related bridge risks. PGN]

Reach Out and Touch Someone...

Henry Cox <cox@spock.ee.mcgill.ca>
Fri, 7 Oct 88 09:00:08 edt

TEENS RUN UP TELEPHONE BILL OF $650 000

[From the Montreal Gazette, 7 October 1988]

LAS VEGAS (AP) - Ten teenage hackers may have run up $650 000 in telephone calls by tricking phone company computers, and their parents could be liable for the tab, authorities said.

"They reached out, all right," assistant U.S. Attorney Russel Mayer said of the hackers, nine 14-year-olds and one 17-year-old. "They reached out and touched the world."

Tom Spurlock, resident agent in charge of the Las Vegas Secret Service office, said the teen agers engaged in "blue boxing," a technique that enabled them to talk to fellow hackers throughout Europe.

"They were calling numbers that were in the ATT system, and their (computer) programs would allow them to `jump' ATT's circuits, allowing them to call anywhere in the world."

The expensive shenanigans came to light when local phone company officials discovered unusual activity on nine Las Vegas phone lines, Spurlock said. He said federal agents obtained warrants and searched the nine homes.

The teenagers weren't taken into custody or charged, but their computers were seized.

Henry Cox

Computer Security and Voice Mail

<davis@community-chest.mitre.org>
Fri, 07 Oct 88 13:35:03 -0400

From the Oct 6 Washington Post.
From a news item "Hackers Find New Way to Tap Long-Distance Phone Lines".

Zotos International Co. received two consecutive $75,000 phone bills, due to use of their automated answering system by hackers.

Zotos' switchboard automatically routes incoming calls to the proper department. Hackers found a way to circumvent the system to place outgoing long-distance calls, in some cases to Pakistan and Senegal. In this case the calls were traced to Pakistani businesses in New York. However, police officials told Zotos that they must catch the hackers in the act in order to prosecute. The telephone company informed Zotos' mangement to pay the bills, and collect from the susspected hackers via the civil courts.

In the same article, a related Los Angeles case of misuse of an electronic switchboard system by outsiders described 'capture' of 200 of a company's password-secured voice mail accounts. Outsiders, in this cases a dope ring and a prostitution ring, gained access by guessing the 4-digit passwords and changing them. The hackers backed off only when 'Federal authorities' began tracing calls.

The article quotes security experts as recommending systems including several access codes. Also, major companies are adding software to detect changes in calling patterns.

Re: Risks of Cellular Phones

Wes Plouff <plouff%nac.DEC@decwrl.dec.com>
6 Oct 88 09:45

Recent writers to RISKS, starting with Chuck Weinstock in issue 7.57, have focused on the risk of vehicle location by cellular telephone systems. In my opinion, they exaggerate this risk and underestimate another risk of mobile phones, the complete lack of privacy in radio transmissions.

Roughly 10 years ago I designed vehicle location controller hardware and firmware used in the Washington-Baltimore cellular demonstration system. That system led directly to products sold at least through the first waves of cellular system construction a few years ago.

Since cellular base stations have intentionally limited geographic coverage, vehicle location is a requirement. This limitation is used to conserve radio channels; one cell's frequencies can be re-used by others far enough away in the same metropolitan area. The cell system must determine which cell a mobile user is located in when he begins a call, and when during a conversation a vehicle crosses from one cell into another. Cells are set up perhaps 3 to 20 miles in diameter and range from circular to very irregular shapes. Cellular phone systems are designed with ample margins so that statistically very few calls will be lost or have degraded voice quality.

Making this system work does not require anything so fancy as triangulation. Vehicle location needs to be only good enough to keep signal quality acceptably high. John Gilmore explained in RISKS 7.58 how this works while the mobile phone is on-hook. During a conversation, the base station periodically measures the signal strength of an active mobile in its cell. When the signal strength goes below a threshold, adjacent cells measure the mobile's signal strength. This 'handoff trial' procedure requires no interaction with the mobile. If the mobile was stronger by some margin in an adjacent cell, both the mobile phone and the cellular exchange switch are ordered to switch to a channel and corresponding phone line in the new cell. Since base stations commonly use directional antennas to cover a full circle, mobiles could be reliably located in one third of the cell area at best. Distance-measuring techniques advocated by AT&T were not adopted because the added cost was too high for the modest performance gain.

Certainly a cellular phone system can locate a mobile at any time, and always locates a mobile during a conversation. But the information is not fine-grained enough to implement some of the schemes imagined by previous writers.

A more important risk is the risk of conversations being intercepted. The public airwaves are simply that: public. Scanner radios can easily be found or modified to cover the cellular band, and listeners will tolerate lower signal quality than cellular providers, hence one scanner can listen to cell base stations over a wide area. The communications privacy law is no shield because listeners are undetectable. To bring this back to risks of computers, automated monitoring and recording of selected mobile phones is probably beyond the reach of the average computer hobbyist, but easily feasible for a commercial or government organization using no part of the infrastructure whatever, just the control messages available on the air.

Wes Plouff, Digital Equipment Corp, Littleton, Mass.
plouff%nac.dec@decwrl.dec.com

Self-correcting (obliterating?) time

Jeffrey R Kell <JEFF@UTCVM.BITNET>
Thu, 06 Oct 88 16:40:32 EDT

I just had a most aggravating experience with a time function which may be

of interest (and this is NOT related to year change, daylight savings time, or any standard horror story). It is machine specific (HP-3000/950).

I have been converting our subroutine library from our old HP-3000 (written in SPL, an obscure systems language for that machine) into 'C' for the new one. One such routine returns the current date in the format we use as a standard database date. I was using ctime() and localtime() functions in the resulting C function. But upon testing, the function was returning a date and time several days and a few odd hours prior to the current date. Extensive testing and tracing revealed that ctime() was not returning the correct clock value; yet all other date references within the operating system were correct. Being more than confused, I placed a problem report.

The cause of the 'bug' was the ctime() library function queries the lowest level hardware clock, and could care less about the operating system clock. This 'feature' came about by porting the C library more or less literally from their Unix-based systems. Although we had set the 'clock' when the system was installed, MPE (the operating system) calculates an offset from the time you 'set' and the hardware clock value, and saves this to set the clock automatically after failures or power outages.

In summary, the hardware clock was never right. MPE tried to correct for this by juggling offsets, thus hiding the real underlying problem. Finally the whole bizarre mess was uncovered by the C library. Needless to say, we have finally correctly set the hardware clock.

Jeffrey R Kell, Dir Tech Services	UTC Postmaster/Listserv co-ord.
Admin Computing, 117 Hunter Hall	Bitnet: JEFF@UTCVM.BITNET
Univ of Tennessee at Chattanooga	JEFF%UTCVM.BITNET@CUNYVM.CUNY.EDU

Risks in ATMs, Parking, Power outages

Steve Philipson <steve@aurora.arc.nasa.gov>
Thu, 6 Oct 88 20:15:54 PDT

This past weekend I got to see/hear about three new RISKS in action.

A friend was in from out of town. She had an interesting story for me. It seems that a bank in New York has a great new feature for their ATM cards: if all you need is an account balance, you can go to a special ATM reserved for that purpose, insert your card, and get your balance immediately. In the interest of saving time, they've made it really simple ... you don't even have to enter your PID (personal I.D. number or password)!!! Veteran RISKS readers can see the folly in this. Of course, on of my friend's office co-workers had her wallet stolen. Inside was both her ATM card and a single blank check. The thief took the card to the ATM machine, found the balance, then made out the check for that amount. Determining liability in this case will be loads of fun.

Next, I drove my friend to San Francisco International Airport for her flight home. I parked in the central parking structure. On entry, you get a

ticket from a machine. The ticket has the time stamped on it in ink, and also a magnetic stripe. The billing mechanism seemed obvious -- read the entry time off the stripe, compute time in the structure, and bill accordingly. It surprised me when the clerk at the exit asked for the correct amount BEFORE I handed him the ticket. Then I noticed that he was facing a TV monitor, and that my car's aft end was on the screen. I asked about the system. It seems that they have another camera and operator enter your license plate number when you enter. They re-enter your plate number as you leave and find the elapsed time between those events. All your comings and goings are recorded. Ain't this a great one! Now big brother can keep track of your comings and goings at the airport. Right to privacy fans might consider public transport as a more private mode of transportation.

[RISKS has had reports before of people being charged for ten days when they parked on two consecutive weekends, and other related horrors. PGN]

Finally, I came into work on Sunday to catch up on a few things.
I had mail! And what did it say? Here's the text, verbatim:

* * * * * * * * * * * * * * * * * * * *

Hi folks. As of 6:13 today, we have completely lost power to N254, our main communications facility. A power transformer feeding that facility appears to have been destroyed (it's all black and burned on the outside, and smells really bad!). While that facility is on UPS, the UPS does not have generator back-up at this time, and as of an hour or so ago, the UPS batteries have been drained. I talked to the power people out there inspecting the transformer, and they said it will be out at least until tommorrow (Monday).

Now, this means all things that depend on N254 are out of service. These include:

All external network access, BARRNET,MILNET,ARPANET,SPAN, etc...
All X.25 access via Telenet.
All ARCLAN access that is attached in the N254 ARCLAN hub, including NAS and N202. [ARCLAN is the Ames Research Center Local Area Net. SHP]
All FTS service to other NASA facilities (at least for now).
[FTS is the Federal Telephone System, our main long distance service. SHP]
All PSCN activities, including TMIS, and ARCNET.

With luck, we'll be back in service as of Monday afternoon or so. The transformer cannot be repaired, so a replacement will have to be found. [FOUND??? No on site spares??? SHP]

Hopefully, this will inspire people to get that generator back-up system funded...

* * * * * * * * * * * * * * * * * * * *

There are lots of folks here at Ames who read RISKS, yet we still have a system with massive losses from failure at a single site. No NASA cracks -- I'll bet this situation is common. Those of you at other sites who are concerned about this kind of thing might show the above to your site managers.
Best of luck.
Steve Philipson

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 63

day 1 October 1988

Contents

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

Re: Killer terminals

Steve Wilson <hplabs!stevew@nsc.nsc.com>
Wed, 5 Oct 88 12:42:58 PDT

After seeing all the articles about Killer terminals I thought I'd relate a story about a killer card reader. Many moons ago I was a computer operator at the local community college. The computer was a Nova 2/10 that spent most of the day running a Basic interpreter talking to 4 ASR-33s. Every afternoon we would bring the Basic system down and run jobs for the Fortran class. We couldn't do this often because the card reader(this was ALONG time ago) would work for about a week, then mysteriously die. We must have had 20 service calls on this card reader over 3-4 month period. Everytime the technician would come out with a new card reader and replace the old one. Finally, the

technician who had to keep on making this weekly trip looked into what was causing the problem. (I'm not sure why he didn't do this the 2nd time the card reader went out, but...) His explanation was that the card reader was "too fast" for the Nova and the real damage was being done by the interface card from the Nova trying to slow the card reader down. They repaired the problem by "turning down" the card reader to a level the Nova could keep up with.

Steve Wilson, National Semiconductor

Can't Happen and Antilock Braking Systems (from Usenet rec.autos)

<Mark Brader <msb@sq.sq.com> [SoftQuad Inc., Toronto]>
Thu, 6 Oct 88 05:54:10 EDT

From: marcus@bbn.com (Marcus Barrow)
Newsgroups: rec.autos
Subject: abs, just say no...
Date: 3 Oct 88 15:40:03 GMT
Organization: Bolt Beranek and Newman Inc., Cambridge MA

I've been seeing this discussion of abs for awhile now, and i have a small story to tell. A friend of mine runs a very modified '87 'vette in the New England Hillclimb series. This car naturally enough has abs, along with oversize rotors, suspension mods and a ~350 b.h.p. smallblock. Abs is probably a "good thing" for many drivers.

But for Mike, " I ain't 'fraid o' no ZR1", there is another story. It seems at Burke Mt. he approached a corner, pushing 90 as he is wont to do. The paved surface at these hills is less than ideal, and the situation is agravated by tripling and quadrupling the speed limit. So the car hit a bump or waver in the pavement and took a skip. Now what does the abs do once the wheels are off the ground? It's not programmed to deal with wheel lockup. It's supposed to prevent that. When four wheels lock up, the unit apparently shuts down for .5 seconds. The pedal stays hard but nothing happens for a terribly long moment...

Mike's car is repairable, but now he's afraid of abs at least!

Marcus@bbn

p.s. please folks, don't try this at home...

-=-= -=-= -=-= -=-= -=-= -=-= -=-= -=-=

From: robert@milk10.uucp (Robert Allen)
Newsgroups: rec.autos
Subject: Re: abs, just say no...
Date: 3 Oct 88 21:43:03 GMT
Organization: SRI International, Menlo Park CA

This isn't the first time this problem has been noted. When abs first became popular some track racers tested it out. Their universal complaint was that when they topped a certain bump in the track, the car lost traction as it became temporarily airborne, and abs interpreted that to mean that abs should be activated since traction was lost.

Computer programs in big computers aren't yet smart enough to
do the instant pattern recognition that the human mind can
apparently make in such circumstances (ie "I haven't REALLY
lost traction yet"), let alone some gimpy program in cars ROM.

- abs. Just say No.

Robert Allen, robert@spam.istc.sri.com, 415-859-2143 (work phone, days)

ATM's credit check

Amos Shapir <amos@taux02.UUCP>
8 Oct 88 21:33:29 GMT

The other night I tried to make a withdrawal of the maximum daily amount allowed. The ATM considered my request, and the said something like: "Service temporarily unavailable", which usually means "I have run out of cash". Trying again later, it insisted that I was no longer allowed to withdraw anything on that business day. As Murphy would have it, I was completely out of cash.

Since all major banks here are tied on the same network, no ATM in town would allow me any credit, and those that can show previous transactions indicated that a withdrawal of the requested amount has been made. This transaction disappeared from the records the next day, and my credit was restored automatically.

It's quite obvious that to save network traffic, the same message from the ATM to the central database which asks for confirmation of credit, also serves to inform it of a withdrawal; it seems that the ATM does not report incomplete transactions. Such sloppiness in programming would not be tolerated in any business, but frankly, my dear, I don't think the banks give a $%^&$@.

Amos Shapir, National Semiconductor (Israel) P.O.B. 3007, Herzlia 46104, Israel
Tel. +972 52 522261

Dive Computers (Re: RISKS-7.60, Brian Randell)

"Terry S. Arnold" <Arnold@DOCKMASTER.ARPA>
Tue, 4 Oct 88 21:07 EDT

The advent of dive computers has changed the way most serious divers go about their sport. Prior to the introduction of dive computers we had to rely on a variety of dive tables based in most cases on originals published in 1959. The current generation of dive computers are based on more current research work on Decompression Sickness and just how nitrogen (the cause of Decompression Sickness) is exchanged during diving. In the past we had to work with our own fudge factors for the artificial dive profiles that the tables assumed. Most divers fudged on the "safe" side were successful in avoiding the bends. The

modern dive computers use a more realistic model of how sport diving is really done and eliminates the need for fudge factors. Like any piece of modern safety equipment dive computer can and are misused sometimes with ill effects. Unlike the usual dive tables the dive computer come with a considerable amount of literature including research references. When I purchased my dive computer I looked up the refrences and read the papers. I found that the dive computers were more conservative than the tables and provided guidance on how to take age, sex, and physical activity into account in a much more realistic way than the guidance published for the dive tables.

I use a dive computer for all of my diving (>200 dives in the last 18 months) and will not dive any other way. I have developed methods so that I can revert back to the tables if a computer failure ever occurs. Most of the reports that I have read in the diving press including the professional association journals indicates that dive computers lead to an overall improved level of safety. The reports that I have seen where divers have suffered from the bends while using dive computers have been strongly correlated with using them to the limits under extreme conditions. In short they were being pushed to the region where the theory was starting to get on thin ground and the tables were just as questionable. This is one case where computers are most likely reducing the risk rather than increasing the risk.

Terry Arnold

Re: Diving Computers

Wed, 5 Oct 88 12:38:24 EDT

>... the computer software may be based on unsafe data, that it does not
>take into account such factors as age, fitness, sex and exertion, and therefore
>gives divers a false sense of security....

I am not a diver, but I am driven to wonder whether the old tables make any real effort to take age, fitness, sex, and exertion into account. It seems much more likely to me that the *real* problem here is not that the software is buggy or unsafe, but that divers are falling into the "computers are always right" trap. That is, everyone knew that the tables were only an approximation to the truth, and used them cautiously, but the supposedly-omniscient computer is not inspiring the same level of distrust.

Another consideration: the computers do (I'm told) take more variables into account. But this isn't necessarily a good thing: since the tables could not do so, they needed safety margins that would accommodate extremes of those variables. That meant that, most of the time, the tables had large safety margins. Divers may well have gotten used to that. It's even possible that those big safety margins were hiding some over-optimistic assumptions, which the software writers have copied.

Henry Spencer at U of Toronto Zoology
uunet!attcan!utzoo!henry henry@zoo.toronto.edu

Emergency Access to Unlisted Telephone Numbers

Dave Wortman <dw@csri.toronto.edu>
Wed, 5 Oct 88 12:35:37 EDT

The article below was originally posted to misc.consumers. I thought it might be of interest to RISKS readers as an example of a well-thought-out set of administrative procedures designed to balance the needs of protection of privacy and response to emergency situations.

==========

All examples in this message pertain to Illinois Bell Telephone Company, which covers the Chicago metropolitan area, and quite a bit of the rest of Illinois.

There are three types of phone numbers which do not appear in the printed and publicly available directory: (1) Too new to list (2) Non-listed (3) Non-pub. [discussion of types (1) and (2) deleted.]

The third category of numbers not in the phone book or available from the Directory Assistance Bureau are non-published numbers. Non-pub numbers are NOT available at the Directory Assistance level. Inquiries about same which are input into a DA terminal simply come up with a message that 'at the customer's request, the number is not listed in our records; the number is non-published.'

Well, who does keep non-pub records then? The Business Office has no handy way to retrieve them, since they depend on an actual phone number when they pull up a record to discuss an account. Once a service order is processed, the number and associated name are no longer available to the average worker in the central office.

There was for several years a small group known as the 'NonPub Number Bureau' which at the time was located in Hinsdale, IL. Needless to say, the phone number to the NonPub Number Bureau was itself non-published, and was only available to specified employees at Bell who were deemed to have a 'need to know'. Now I think with all the records being highly computerized, the keepers of the non-pub phone numbers are themselves scattered around from one phone office to another.

When there is some specific need for an employee at the phone company to acquire the non-published number of a subscriber, then certain security precautions kick into place. Only a tiny percentage of telephone company employees are deemed to have a 'need to know' in the first place; among these would be the GCO's (Group Chief Operators), certain management people in the central offices, certain people in the Treasury/Accounting office, and of course, security representatives both from Illinois Bell and the various long distance carriers, such as AT&T/Sprint/MCI.

Let us have a hypothetical example for our Correspondent: Your mother has taken seriously ill, and is on her deathbed. Your brother is unable to reach you to notify you of this because you have a non-pub number. When his request for the number has been turned down by Directory Assistance, simply because they do not have it, he asks to speak with a supervisor, and he explains the problem. He provides his own name and telephone number, and the supervisor states he will

be called back at a later time. The supervisor does not question if in fact an emergency exists, which is the only valid reason for breaking security. The supervisor may, if they are doing their job correctly, ask the inquirer point blank, "Are you stating there is an emergency situation?".

Please bear in mind that the law in Illinois and in many other states says that if a person claims that an emergency exists in order to influence the use (or discontinuance of use) of the telephone when in fact there is no emergency is guilty of a misdemeanor crime. You say yes this is an emergency and I need to contact my brother/sister/etc right away. The supervisor will then talk to his/her supervisor, who is generally of the rank of Chief Operator for that particular facility.

The Chief Operator will call the NonPub people, will identify herself, and *leave her own call back number*. The NonPub people will call back to verify the origin of the call, and only then will there be information given out regards your brother's telephone number. It helps if you know the *exact* way the name appears in the records, and the *exact* address; if there is more than one of that name with non-pub service, they may tell you they are unable to figure out who it is you want.

The NonPub person will then call the subscriber with the non-published number and explain to them what has occurred: So and so has contacted one of our operators and asked for assistance in reaching you. The party states that it is a family emergency which requires your immediate attention. Would it be alright if we give him/her your number, *or would you prefer to call them back yourself?*

Based on the answer given, the number is either relayed back to the Chief Operator, or a message is relayed back saying the non-pub customer has been notified. If the customer says it is okay to pass his number, then the Chief Operator will call you back, ask who YOU are, rather than saying WHO she wants, and satisfied with your identification will give you the number you are seeking or will advise you that your brother has been given the message by someone from our office, and has said he will contact you.

Before the NonPub people will even talk to you, your 'call back number' has to be on their list of approved numbers for that purpose. A clerk in the Business Office cannot imitate a Chief Operator for example, simply because NonPub would say that the number you are asking us to call back to is not on our list. "Tell your supervisor what it is you are seeking and have them call us..."

Other emergency type requests for non-pub numbers would be a big fire at some business place in the middle of the night, and the owners of the company must be notified at their home; or a child is found wandering by the police and the child is too young to know his parent's (non-pub) number.

They will also handle non-emergency requests, but only if they are of some importance and not frivolous in nature. You have just come to our city to visit and are seeking a long lost friend who has a non-pub number; you are compiling the invitations to your high school class fiftieth re-union and find a class member is non-pub. Within certain reasonable limits, they will pass along your request to the desired party and let them make the choice of whether to return the call or not. But always, you leave your phone number with them, and in due

time someone will call you back to report what has been said or done.

You would be surprised -- or maybe you wouldn't -- at the numerous scams and [.....] stories people tell the phone company to get the non-pub number of someone else. Fortunately, Bell takes a great deal of pride in their efforts to protect the privacy of their subscribers.

Patrick Townson, The Portal System(TM)
uunet!portal!cup.portal.com!Patrick_A_Townson

Re: Risks of Cellular Phones

Wes Plouff <plouff%nac.DEC@decwrl.dec.com>
6 Oct 88 09:45

Recent writers to RISKS, starting with Chuck Weinstock in issue 7.57, have focused on the risk of vehicle location by cellular telephone systems. In my opinion, they exaggerate this risk and underestimate another risk of mobile phones, the complete lack of privacy in radio transmissions.

Roughly 10 years ago I designed vehicle location controller hardware and firmware used in the Washington-Baltimore cellular demonstration system. That system led directly to products sold at least through the first waves of cellular system construction a few years ago.

Since cellular base stations have intentionally limited geographic coverage, vehicle location is a requirement. This limitation is used to conserve radio channels; one cell's frequencies can be re-used by others far enough away in the same metropolitan area. The cell system must determine which cell a mobile user is located in when he begins a call, and when during a conversation a vehicle crosses from one cell into another. Cells are set up perhaps 3 to 20 miles in diameter and range from circular to very irregular shapes. Cellular phone systems are designed with ample margins so that statistically very few calls will be lost or have degraded voice quality.

Making this system work does not require anything so fancy as triangulation. Vehicle location needs to be only good enough to keep signal quality acceptably high. John Gilmore explained in RISKS 7.58 how this works while the mobile phone is on-hook. During a conversation, the base station periodically measures the signal strength of an active mobile in its cell. When the signal strength goes below a threshold, adjacent cells measure the mobile's signal strength. This 'handoff trial' procedure requires no interaction with the mobile. If the mobile was stronger by some margin in an adjacent cell, both the mobile phone and the cellular exchange switch are ordered to switch to a channel and corresponding phone line in the new cell. Since base stations commonly use directional antennas to cover a full circle, mobiles could be reliably located in one third of the cell area at best. Distance-measuring techniques advocated by AT&T were not adopted because the added cost was too high for the modest performance gain.

Certainly a cellular phone system can locate a mobile at any time, and always

locates a mobile during a conversation. But the information is not fine-grained enough to implement some of the schemes imagined by previous writers.

A more important risk is the risk of conversations being intercepted. The public airwaves are simply that: public. Scanner radios can easily be found or modified to cover the cellular band, and listeners will tolerate lower signal quality than cellular providers, hence one scanner can listen to cell base stations over a wide area. The communications privacy law is no shield because listeners are undetectable. To bring this back to risks of computers, automated monitoring and recording of selected mobile phones is probably beyond the reach of the average computer hobbyist, but easily feasible for a commercial or government organization using no part of the infrastructure whatever, just the control messages available on the air.

Wes Plouff, Digital Equipment Corp, Littleton, Mass.
plouff%nac.dec@decwrl.dec.com

Re: Risks of cellular telephones

Peter Robinson <pr@computer-lab.cambridge.ac.uk@NSS.Cs.Ucl.AC.UK>
28 Sep 88 10:10:47 +0100 (Wednesday)

As a radio amateur, I have always been taught that using mobile transmitters near petrol stations is bad form - the radiation from the transmitter can induce currents in nearby metalwork and perhaps cause a spark. The thought of a cellular telephone being able to transmit without the operator's consent (in response to a paging call) is, therefore, slightly RISKy.

This could even get worse as technology progesses. As the sunspot cycle advances, it seems plausible that transmissions will carry further and interfere with those in nearby cells (not the adjacent ones, they usually have distinct frequencies). Before long the manufacturers will introduce adaptive control where the transmitter power is adjusted dynamically to compensate for variations in the signal path between the mobile and base stations. So then when you pull into a petrol station and receive a call, the system will notice that all the surrounding metal is impairing your signal and will increase the transmitter power accordingly...

Incidentally, I am not sure what power these radios use, but I would be slightly nervous about using a hand-held telephone with the antenna anywhere near my eyes if it is more than a few Watts.

Risks of cellular phones

"Walter Doerr" <wd@dg2kk.UUCP>
Sat, 8 Oct 88 15:59:56 MET

Chuck Weinstock <weinstoc@SEI.CMU.EDU> writes in RISKS 7.57:

> Subject: Risks of Cellular Phones?

>
> While discussing radio triangulation last night, the question came up:
> If I dial a phone number attached to a cellular phone, how does the
> cellular system know which cell should send the ring signal to the
> phone? Is it a system wide broadcast, or does the cellular phone
> periodically broadcast a "here I am" signal?

In the 'C-Net' here in Germany, all mobile phones send a "here I am" signal whenever they move to a new cell. This information (the cell where the phone can be reached) is stored in the database of the phone's "home" base. Calls to mobile phones are routed to a computer in Frankfurt which contacts the home base computer (based on the first few digits of the mobile phonenumber), which, in turn, knows the cell the phone is currently in.

> If the latter, a less than benevolent government (or phone company for
> that matter) could use that information to track its citizens' cars'
> whereabouts.

According to an article in an electronics magazine, the German PTT was approached by a police agency, who expressed interest in the data stored in the networks computers. The article quotes a Siemens mobile telephone specialist as saying that it isn't possible to pinpoint the current location of a mobile phone because:

- the phone must be switched on for the network to recognize it
- the cells use omnidirectional antennas, so it isn't possible to determine the direction from where the mobile phone's signal came.

While this is true, it is certainly possible to determine the location of a phone with an accuracy of a few miles (the size of the cell the phone is in) without using any additional direction finding methods (radio triangulation).

Walter Doerr

Computers, Copyright Law, and the Honor System (a talk)

Mark Mandel <Mandel@BCO-MULTICS.HBI.HONEYWELL.COM>
Mon, 10 Oct 88 09:47 EDT

"ARE WE ALL ON THE HONOR SYSTEM?":
Computers, Copyright Law, and the Honor System
Mark A. Fischer, of counsel to the firm of Wolf, Greenfield & Sacks Boston

Easy access to information through computer databases has given tremendous power to people once called readers -- now known as "end-users." The change in title is significant. End-users have the power to reproduce, store, transmit, and use information once reserved to publishers. Are the legal obligations coincident with the ethical? Are the legal obligations enforceable? Are we all on the honor system?

Mr. Fischer represents publishers, software firms, musicians, authors, performing artists, and theatrical and motion-picture producers. He holds a

law degree from Boston College Law School and specializes in copyright, publishing, entertainment, arts and computer law. He has taught courses in Copyright and Trademark Law and in Intellectual Property. His writing has appeared in BILLBOARD, the JOURNAL OF THE COPYRIGHT SOCIETY, and ANIMAFILM. He is a member of the American Bar Association's Forum Committee on the Entertainment and Sports Industries, and chairman of the Boston Patent Law Association's Copyright Law Committee.

WEDNESDAY, 19 October 1988
7:30 P.M.
8th floor lounge, 545 Technology Square, Cambridge
(Corner of Main & Vassar Streets, in Kendall Square)
Free parking in front

SPONSORED BY COMPUTER PROFESSIONALS FOR SOCIAL RESPONSIBILITY
CPSR/Boston * P.O. Box 962 * Cambridge, MA 02142 * 617-666-CPSR

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 64

Thursday 1 October 1988

Contents

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

---

100 digit primes no longer safe in crypto

davy@riacs.edu <David A. Curry>
Wed, 12 Oct 88 20:34:01 -0700

Taken from the San Jose Mercury News, Oct. 12, 1988, Page 8A:

Computers able to make light work of cracking code (Los Angeles Times)

Some secret codes intended to restrict access to military secrets and Swiss bank accounts may not be as safe as had been presumed, a team of computer experts demonstrated Tuesday.

The team succeeded in doing what security experts thought could not be done:

using ordinary computers to break down a 100-digit number into the components that produce it when multiplied together.

That process, called factoring, holds the key to many security codes.

Before Tuesday, experts had believed that if the number was large enough - up to 100 digits - its factoring would take about 10 months with a Cray super-computer, one of the most powerful computers in the world.

But computer experts across the United States, Europe and Australia solved the problem more quickly by using 400 processors simultaneously. They linked their computers electronically and factored a 100-digit number in just 26 days.

The number has two factors, one 41 digits long and the other 60 digits long.

And that, according to Arjen Lenstra, professor of computer science at the University of Chicago, should be quite sobering to experts who believe they are secure with codes based on numbers that large. Lenstra headed the project, along with Mark S. Manasse of the Digital Equipment Corp.'s Systems Research Center in Palo Alto.

[quotes from experts]

Rodney M. Goodman, associate professor of electrical engineering and an expert on cryptography at the California Institute of Technology in Pasadena, described the achievement as "significant," because it means that some systems may not be as secure as had been thought. But he said it did not mean that security experts around the world would have to rebuild their systems.

"All the cryptographers will do is increase the length of the number by a few more digits," he said, "because the problem gets exponentially worse as you increase the size of the number." A larger number is more cumbersome, and cryptographers had tried to kep the number as small as possible.

[explanation of the idea behind using large numbers with
prime factors in cryptography]

Last year, Lenstra decided to tackle the problem on "a small scale, just to see if he could do it," according to Larry Arbeiter, spokesman for the Univ-ersity of Chicago. "It was a pure science type of effort."

Several months ago, Lenstra presented his idea to Manasse, a computer re-search scientist with Digital. Manasse became so intrigued with the problem that his company agreed to fund much of the cost, including the use of more than 300 computer processors at the Palo Alto company during off-duty hours. The company manufactures DEC computers.

"I was interested in the general problem of taking a program and breaking it up into small pieces" so that many could work simultaneously toward the sol-ution, Manasse said.

Other computer enthusiasts from the "factoring community" clamored aboard and this fall more than 400 computers around the globe were ready to give it a try.

The computers ranged in size from microcomputers to a Cray supercomputer, but even personal computers with large memories could have been used, Lenstra said. Each of the participating computers was given a different part of the problem to solve, and success came early Tuesday morning.

Risks of computer controlled doors

Piet van Oostrum <piet@ruuinf.UUCP>
12 Oct 88 11:20:12 GMT

Amsterdam, The Netherlands

The new Amsterdam Stopera (combined town hall - music theater) has to undergo $1 million of upgrading, although it is only a few years old. One of the things to be done is redoing the computers controlling the doors, as several people have had the experience of being locked up.

Piet van Oostrum, Dept of Computer Science, University of Utrecht
Padualaan 14, P.O. Box 80.089, 3508 TB Utrecht, The Netherlands
Telephone: +31-30-531806 UUCP: ...!mcvax!ruuinf!piet

NSFnet Backbone Shot

Gene Spafford <spaf@purdue.edu>
12 Oct 88 19:14:22 GMT

The following mail was forwarded to me a few minutes ago. This refers to the MCI fiber used to carry the NSFnet backbone. No wonder some of my mail has disappeared recently! [From: field inadvertently deleted?]

=> Date: Wed, 12 Oct 88 12:47:00 EDT
=> To: watchdogs@um.cc.umich.edu, ie@merit.edu
=> Subject: A bit of trivia
=>
=> The fiber that goes from Houston to Pittsburgh was broken due
=> to a gun blast....that is right, a gun blast.
=> Somewhere in the swamps of the Bayou (between Alabama and New Orleans)
=> the fiber cables are suspended above the swamps and a good ol'
=> boy was apparently target practicing on the cable.
=>
=> Traffic has been rerouted and when the investigation has taken place
=> and the cable fixed we will be put back on the original circuit.

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

Intersection of ANI and Voice Mail Risks

<MCCLELLAND_G%CUBLDR@VAXF.COLORADO.EDU>
Tue, 11 Oct 88 00:14 MDT

Recent reports in RISKS of nefarious deeds committed by hackers who entered a system via voice mail prompted me to inquire about the voice mail security of my university's system. A year ago the U bought its own fancy switch for on-campus communications. Some of the goodies include voice mail and ANI. I tried the voice mail once but since I much prefer e-mail

I long ago forgot my voice mail password (yep, only 4 digits if the hackers want to start guessing). I called the telecommunications office to determine where I needed to go in person and with how many photo ID's to get my voice mail password. Even though I hadn't identified myself, the clerk said, "Oh that won't be necessary, Mr. McClelland, I'll just change your password back to the default password and you can then change it to whatever you want." I said, "But how do you know that I'm McClelland?" He replies, "Because it shows on the digital display on my phone both the phone number and name of the caller." [Most phones are in private offices so a unique name can be attached to each number.] I tried to explain that all he really knew was that I was someone calling from the phone in McClelland's office and that I could be the janitor, a grad student, or almost anyone. But security wasn't his problem so he wasn't very concerned. I was afraid to ask how many folks never bother to change their default password. As I was about to hang up, he said, "By the way, if you check your voice mail from your own extension you don't even need to enter your password." I said , "Thanks, that's reassuring" but I don't think he caught the sarcasm.
Gary McClelland

New Feynman book

Eugene Miya <eugene@amelia.nas.nasa.gov>
Wed, 12 Oct 88 23:41:09 PDT

I remembered that many fans of RISKS are also Richard Feynman fans.
I ran into Stacey's briefly today and just happened to see this:

%A Richard P. Feynman
%T "What Do YOU Care What Other People Think?"
%I W. W. Norton
%C New York
%D 1988
%$ 18

Relevance to RISKs readers comes in two forms (his essay on the Value of Science at the end and the appendix to the Challenger report which makes up over 50% of the book). Note that the text is longer and not verbaum to the articles in Engineering and Science or Physics Today.

--eugene miya, NASA Ames

High `Rev'ing Volvo

<hartel@mitre.arpa>
Tue, 11 Oct 88 10:10:15 EDT

I have an old disreputable '82 Volvo which gave me an object lesson in sensor circuit design recently. Beginning several months back the car began to exhibit a mind of its own about engine speed. The local ace Volvo dealer couldn't find anything wrong after $400 worth of effort, and since the car's

independence of mind seemed to be limited to brief and infrequent periods, I let the matter slide. Poor idea. I took the car to the wilds of northern Wisconsin, far from the nearest Volvo fixit shop, where the old car turned on me. Previously my problems with engine speed had been limited to surges in speed at idle, up to no more than 2500 RPM. There had been no signs of bad behavior when the car was in gear. Once up in the great frozen north however, the car decided it was going to idle at fifty MPH, as in 2700 RPM in fourth gear up a hill. Kept doing it too. Made it hard to drive thru the camp ground, observe nature, stay alive.

I studied the owner's manual. It has an elementary schematic of the fuel system, and one particular element which caught my eye was the constant idle control, a servo motor that appeared to affect manifold vacuum. Got inputs from several sensors and the engine microprocessor. When I disconnected the control, idle dropped to nominal, and the car was drivable.

In the end the Volvo dealer found the problem, which was that a spade connector had come adrift from one of the engine sensors. The idle control interpreted lack of signal from the sensor as low engine speed, so it exerted its maximum effort to raise the idle speed to acceptable levels. It strikes me as poor design that an open circuit mimics the operative signal in a sensor system. Automotive engine compartments are well knows as hell on earth for electronics, and loose connections and broken wires are to be expected. Lack of signal should cause the automated system to go off line, not off its head.

Stevie Wonder gives an Ear-itating Performance

mjj@stda.jhuapl.edu (Marshall Jose) <@aplvax.jhuapl.edu:mjj@ ...>
Tue, 11 Oct 88 11:06:37 EDT

The following is regrettably anecdotal and I wish I had more firsthand info on it; anyway, here goes:

For one of his tours, Stevie Wonder contracted with Northwest Sound to build a set of PA speakers of extraordinary capability -- response nearly flat out to 45 kHz, etc. A few weeks into the tour, though, the performances seemed to be souring. Everybody -- artists, crew, even the audience -- seemed irritable and impatient. Indeed, the performances started out well enough, but an hour or so into the show the audience became testy and actually were moved to boo during pauses, for no apparent reason.

Finally, during one show, one of the sound guys was examining the audio spectrum analyzer screen, and mistakenly pushed the 20 kHz - 200 kHz range button instead of the 2 kHz - 20 kHz button. Imagine his alarm at the sight of a potent 28 kHz component, the product of all the synthesizers' DAC update clocks. It was lying just outside the (ordinarily) high hearing limit of 20 kHz, so it was never noticed by the sound crew and their instrumentation. Cause discovered, the noxious 28 kHz spike was eliminated with an equalizer, and everybody went home happy but chastened.

The person who related this story to me suspects that the event is not widely known, being of large embarrassment and trivial cause. Is he right? Has anyone else heard about this?

Ear-itation

Peter G. Neumann <Neumann@KL.SRI.COM>
Wed, 12 Oct 88 15:00:28 PDT

I am reminded of the not-computer-related experience of the Columbia professor who noticed that his body went limp in a record store whose speakers were blaring a particular rock tune. He took the record back to his lab and analyzed it -- discovering some sort of a alpha- or beta-wave resonant frequency with the human brain of his students, for that particular rhythm -- an AN-A-PEST with the accent on the last syllable -- DA-DA-DUM. It was many years ago, but still worth relating for the younger folks who like to listen to hard-beat music... Beware of the anapest.

OMB "Blacklist"?

Hugh Miller <@CORNELLC.CCS.CORNELL.EDU:HUGH@vm.utcs.utoronto.ca>

The following appeared in the 1987 annual report of Project Censored, a U.S. group operating out of Sonoma State University. They compile an annual list of what they consider to be the 25 most un- or under-reported stories of the year. This is #22 on the latest hit parade. The collection is widely available on local RCPM's; the one I pulled down was labelled CENSOR.ARC. [Hugh Miller, University of Toronto, (416)536-4441]

OMB COMPILING NATION-WIDE BLACKLIST OF GRANT VIOLATORS

The Office of Management and Budget is compiling a master computer list of those debarred or suspended from participating in government agency grant programs. Gary Bass, executive director of OMB Watch, a public interest group that monitors the budget office, said the goal of reducing waste, fraud and abuse is laudable but warned that the program "can become a hit list for individuals and organizations that the administration does not agree with."

The controversial program will cover a wide range of transactions, including grants, cooperative agreements, scholarships, fellowships, loans and subsidies. It would apply to both recipients of federal funds and those "doing business" with them. The system is expected to be fully operational by May, 1988.

Under the new law (Reagan's Executive Order 12549), 20 agencies which disburse $100 billion in grants will forward their debarred lists to the OMB. The master list will be computerized and placed on a nation-wide automated telephone system. Regulations published in the Federal Register (5/29/87) say that the master list will contain names and "other information" about currently debarred or suspended grant recipients, as well as about those whose debarment is pending.

Under the directive, federal, state and local agencies, private organizations and individuals handling federal funds must check the list before providing anyone a federally-aided service, grant, loan or other assistance such as day care. Any person or organization that fails to check the list may also be placed on it. In addition, employees of federally-funded agencies and organizations, as well as anyone "doing business" with them or wishing to do business with them must submit annual certifications that neither they nor anyone "associated with" them are on the list, or being considered for it.

Grounds for placement on the list include 1) violating any term of a "public agreement," regardless of whether federal funds were involved; 2) failure to repay a government-backed or assisted loan, such as a home mortgage, student or crop loan; 3) "failure to perform" or poor performance on a grant or other "public agreement;" 4) lack of "business integrity or honesty" or conviction of "business" crimes; 5) debarment or suspension by a public agency at any level of government, federal, state, or local.

One can also make the blacklist if one: is a public school teacher and goes on strike despite a no-strike clause in one's contract; performs poorly on any grant from a public agency, regardless of whether federal funds were involved; does business with anyone known to be on OMB's new list.

Various agencies already keep records of those who violate rules of grants, using the lists to prevent such recipients from getting additional grants from the agency involved. But, under current law those same recipients may obtain grants from other federal agencies.

Rep. Jack Brooks (D-TX), chair of the House Government Operations Committee warned that the OMB's implementing guidelines "endorse guilt by association, reverse the presumption that a person is innocent until proven guilty, and define the operative offenses so vaguely as to potentially encompass many entirely legitimate activities."

SOURCES: THE NEW YORK TIMES, 12/23/87, "U.S. Plans to Make Master List ...", by Martin Tolchin; OMB WATCH 1987 ANNUAL REPORT; FOUNDATION NEWS, July/August 1987, page 8.

Re: Ethics of Conflict Simulation

wilde@hor-res.UUCP <@RELAY.CS.NET:hor-res!wilde@gte.com>
Mon Sep 26 15:08:41 1988

In RISKS-FORUM 7.55, Mike Trout makes several statements regarding the past and present state of the conflict simulation industry. While I do not wish to digress too far from the purpose of this list, I feel that the picture he presents is somewhat inaccurate.

The main issue confronting game designers doing work for the military is one of integrity, as Mike pointed out. The problem is not some nebulous fear of the Pentagon "poisoning" the industry as a whole, but rather

that they would interfere _with the particular game under consideration_. The designers want to be free to model a situation as they see it. The military, however, gets upset when someone gives them a simulation that says their high tech weapons have an expected lifetime of 3 minutes in actual combat. As a result, most designers will not consider working for the govt. unless they are assured of complete freedom in doing their designs.

As for Pentagon influence "subverting" the game industry, I have yet to see any indication that anything more than a small fraction of game designers and publishers revenues come from military contracts. Many games have been produced dealing with hypothetical modern conflicts, but I believe this is a reflection of the interests of gamers , not the result of some sinister military infiltration. I definitely feel there is no justification for saying these games were developed to find "better ways to slaughter people". Only a handful of games on the market were originally developed as simulations for the military.

Mike's statement about having fun is somewhat puzzling. These designs are _GAMES_. Most people play them for the enjoyment of intellectual competition. They also play them to more fully understand history (and future possibilities). The two are not incompatible goals.

Scott Wilde ...bunny!hor-res!wilde

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 65

Saturday 15 October 1988

Contents

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

Vendor introduces "safe" Ada subset

jon@june.cs.washington.edu <Jonathan Jacky, University of Washington>
Fri, 14 Oct 88 09:04:38 PDT

From ELECTRONIC ENGINEERING TIMES, 26 Sept 1988, p. 25:

Ada SUBSET ADDRESSES SOFTWARE SAFETY

Southampton, England - (A subset of Ada called Spark) is reported to overcome the drawbacks of (Ada) in applications where software integrity is critical. ... Spark was developed at the University of Southampton with the sponsorhip of the British Ministry of Defence. It is now being marketed by Program Validation Ltd.

(A representative of Program Validation) said that the use of Ada for safety critical programming poses some serious problems. There is no formal definition of the language and the precise meaning of some its constructions is unclear. According to Program Validation, the resulting uncertainties make formal verification of Ada programs impossible and cast doubts on the integrity of the compiled code. A further complication is that the richness of Ada

allows programs to be constructed that are apparently simple, but hide great underlying complexity.

... To achieve Ada integrity, Spark has introduced several restrictions. It does not allow the use of tasks, exceptions or generic units. Access types are also omitted, as these are considered unacceptable in real-time safety critical applications. ... Certain features - such as "go to" statements and "declare" statements - are totally barred.

Re: ethics of conflict simulation

Sean Malloy <malloy@nprdc.arpa>
Thu, 13 Oct 88 13:40:12 PDT

>From RISKS-FORUM 7.74: (Scott Wilde) The problem is not some nebulous
>fear of the Pentagon "poisoning" the industry as a whole, but rather
>that they would interfere _with the particular game under consideration_.

In fact, one of the games designed by Simulations Publications, Inc. (SPI) before they were bought out by TSR was _ordered_ by the Army. _Firefight_ was intended as a simulation for warfare in Europe, to teach tactics to infantry and armor commanders. Within a number of simplifying abstractions, it modeled the weapons systems available to a unit commander in Germany.

SPI later made this game available as part of their regular line. It soon became apparent that the game was not only useful for teaching tactics, it was also a device to build confidence and improve morale -- the way the rules and weapons systems data were set up, it was almost impossible for a Soviet player to pull anything better than a draw out of the game. The game mechanics were biased so that an American player could win by using the `right' tactics (`right' in the Army sense -- the approved Army tactics for a given situation), rather than encouraging the players to come up with their own tactics.

>From the Army's point of view, it was a very good simulation. From the opinions expressed about it in the gaming community, it flopped miserably as a _game_.

Sean Malloy, Navy Personnel Research & Development Cntr, San Diego CA 92152-6800

Re: Assault on Privacy

Ronni Rosenberg <ronni@VX.LCS.MIT.EDU>
Thu, 13 Oct 88 13:36:10 edt

Thanks to Anthony Atkielski for providing information on privacy legislation in France. I hope that France's legislation closes some of the loopholes in U.S. privacy legislation. But it is worth pointing out that laws that may sound good on the books often do not translate into tough action.

For instance, the Fair Credit Reporting Act (1971) specifies expiration periods, for bankruptcy data (14 years) and other adverse data (7 years),

which is not well defined. Where legislation contains vague definitions, applying it may be left to the judgement of the agency being regulated.

The FCRA also requires credit agencies to provide you with the data in their file about you, on request, and to allow you to correct it. Sounds good. But you can get such info. for free only after you have been denied credit on the basis of it. If you want to get the info. before you have a problem, it's not too expensive, but you'll have quite a time trying to find all the private organizations that maintain files about you. If you make a correction, there is no guarantee that it will be propogated to other files based on this one and to other organizations that obtained the false data previously. And if you lost something, such as a mortgage, because of false data, tough luck.

The Privacy Act (1974) makes it easier for people to know about their files (in government agencies and the private organizations with which they do business). But publication of the existence of records is done in the Federal Register, which is not exactly handy.

Agencies are restricted from releasing personal data to another agency without written permission of the person who provided the data, except for "routine" purposes. In 1979, the Office of Personnel Management released lots of its data to other agencies. What was the "routine" purpose? "To protect the legitimate interests of government." Similar definitions can be used to "justify" the collection of any sort of info.

Atkielski thinks that individuals in France can insist that a credit bureau erase its file about themselves. But if society is structured so that many of the normal transactions of life depend on credit ratings, how real a "choice" do you have about participating?

I wish much more of the burden were on the organizations that maintain (and, in many cases, profit from) data banks. I'd like to see organizations held responsible for notifying individuals directly about the existence of files about themselves; requesting permission from individuals every time info. is released; guaranteeing that corrections will be made and propogated quickly; assuming liability for losses based on false data; and so on.

Software warranties and Trade Practices in Australia

Lee Naish <lee@munmurra.mu.oz.au>
Wed, 12 Oct 88 13:43:36 EST

> [This was picked off the net in Australia, from "cbp",
> including and commenting on a letter from B L COOMBS. Lee]

Software Warranties - The Truth

[The Trade Practices Commission recently sent the following letter to 2000 Australian computer companies.

Permission has been obtained from Ian Searle of the TPC to reproduce this letter here

<

RISKS of EPROMS

George Sukenick <sukenick%ccnysci%cucard@nyu.edu>
Mon, 10 Oct 88 15:35:08 EDT

> RISKS of EPROMS (Daniel Klein)
>The UV eraseable EPROMS that are found in many smaller computers are also
>subject to failure when their picture is taken. Yep, you read that correctly.

(Due to camera shy EPROMS? :-))

Electronic flashes draw a lot of current in a short time. The unshielded system might have been crashing due to EMP rather than light interfering with the EPROMs. I guess that the test would then be to see what happens with various combinations of covering the EPROM's windows (they were open in the machine?) and shielding the flash.

-george

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 66

Thursday 20 October 1988

Contents

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

British computer calls Northern Ireland a "Region Unknown"

John Murray <johnm@amdahl.uts.amdahl.com>
20 Oct 88 18:25:36 GMT

Paraphrased from The Irish Times (Dublin), Oct 15 1988:

'A computer error resulted in the gross domestic product of Northern Ireland being underestimated by more than 10 percent between 1983 and 1986. [A spokesperson for the Northern Ireland Economic Council] said that the sluggishness evidenced by the statistics "could have undermined the confidence of potential investors".'

. . . . 'Over 70 percent of the North's GDP consists of estimates of income [which] are calculated at Newcastle-on-Tyne [England] from income tax returns and information in the Dept. of Health & Social Services. It appears that between 1983 and 1986 an error in the computer programme responsible for extracting the relevant data categorised a growing number of earners in the North as "region unknown".'

[Further discussion follows about how the error may have supplemented

the region's other problems.]

"Brain" virus shows up in Hong Kong

Dave Horsfall <dave@stcns3.stc.oz.au>
Tue, 18 Oct 88 13:34:27 est

On the off-chance that you haven't had enough of virus reports, here's another one from Computing Australia, 17th October, 1988:

``HK consultants hit by overseas virus

> A leading firm of financial consultants has become the first main-stream business in Hong Kong to be affected by a computer virus. The Business International consultancy reported last week the "Brain" virus -- well-known elsewhere in the world, but never before seen in Hong Kong -- had appeared on some disks. ... BI was playing down the significance of the find last week, with a company spokeswoman saying the virus had not reappeared and that no data had been lost.''

The article goes on further to discuss the origin of the Brain virus, and makes the amazing observation "[it] does not destroy data, but scrambles it beyond recognition". I dunno, I would certainly regard data "scrambled beyond recognition" as being "destroyed".

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

A Credit Card Fraud

Brian Randell <B.Randell@newcastle.ac.uk>
Tue, 18 Oct 88 11:51:07 +0100

This story, from Saturday's Guardian newspaper, comes from what sounds like an interesting study of computer-related crime. It is reprinted here in full, without permission. (The # sign is used to represent the pounds sterling sign.) The risk in the particular fraud described would appear to have arisen - said he with 20:20 hindsight, but no personal expertise in credit card fraud - because of the latencies in, and inadequacies of, the means by which input validity checks were performed.

Brian Randell

#9M Credit Card Fraudster Cleans Up With a Full House

[by] Peter Large
Technology Editor
[Guardian, 15 Oct. 1988, p.11]

Credit card companies were robbed of #6 million to #9 million within two weeks

by an eight stage, one-man fraud. The recipe used was this:

1: Take a mortgage on a house that has already changed hands once in the past five years.

2: Advertise a bogus job overseas at a juicy salary (that brings 4,000 replies).

3: Send the job applicants a form demanding the same details as those required for a credit-card application.

4: The hard work: transfer that information to the application forms of several smallish credit-card and store-card operators, forging the signatures and substituting the address of the safe house for the real address (that ensures that any check with the electoral roll draws a blank, without indicating a bogus applicant).

5: The fast work: spend or draw cash to the maximum possible - and within one day - on each card as it arrives at the safe house.

6: To outpace the tracing, complete the operation within two weeks, even though there are still many cards to spare.

7: Disappear.

8: Don't pay for the advert.

The case - he was never caught - was reported yesterday in the BIS group's annual study of computer-related crime. Bill Farquhar, co-author of the report, said the crime was discovered, much too late, when a clerk entering details into a computer noted the same handwriting on different applications from the same address.

Mr Farquhar said #3 million was traced from bank to building society to another bank, before it was transferred abroad. But the total take was at least #6 million and probably #9 million, he said. The police found an empty house carpeted with cards.

The report shows how computer fraud is spreading: the 225 cases traced by BIS in the past year netted an average of #389,000, compared with #31,000 in 1983. BIS reckons 90 per cent of computer crime is not reported by firms - or not traced at all.

Firms so fear the publicity that some give the criminals golden handshakes and glowing references to pass on to their next victim."

[Also noted by blf@scol.uucp]

Nausea-inducing propeller (Re: RISKS DIGEST 7.64)

Mike Trout <miket@brspyr1.brs.com>
17 Oct 88 18:35:47 GMT

In RISKS-FORUM Digest Volume 7 : Issue 64, Marshall Jose discusses how an unwanted 28 kHz spike at a Stevie Wonder tour was inducing irritability and impatience among artists, crew, and audience. Our illustrious moderator Peter also mentioned how the anapest beat of a particular rock tune could cause alarming physical effects on certain people.

This brings to mind the story of the infamous XF-84H, an airplane whose tale appears every now and then in rec.aviation. You may remember the old F-84 Thunderstreak/flash/whatever; in those days jet engines left a great deal to be desired in both maximum power output and reliability. Accordingly, somebody got the bright idea of putting a super turboprop on the front of an F-84. Tests showed the plane (designated the XF-84H) to have lots of reliable power and acceleration, but there was an unexpected side effect nobody predicted: ground crews working with the XF-84H began suffering from uncontrollable nausea. The cause was traced to the plane's monstrous propeller blades, which of necessity were spinning at supersonic speeds and apparently setting up some physiologically harmful harmonics. The project was scrapped; the only XF-84H built is on display at some AFB in California, I believe.

There seems to be little hard data in circulation about this project; it is mentioned briefly in various authoritative publications but the details are always sketchy. Some questions that come to mind: What kind of harmonics would induce nausea, rather than something like irritability as in the Stevie Wonder 28 kHz spike? Why was the pilot apparently not affected? Why is nausea NOT induced by other supersonically-spinning propellers (which occasionally crop up on various general aviation aircraft)? I'm sure that USAF and Republic Aviation reports on this incident exist somewhere; anybody know any more?

Michael Trout (miket@brspyr1)~~~~~~~~~~~~~~~~~~~~~~~~~
BRS Information Technologies, 1200 Rt. 7, Latham, N.Y. 12110 (518) 783-1161

Re: Ear-itating performance

<wolit@research.att.com>
Mon, 17 Oct 88 08:59 EDT

> For one of his tours, Stevie Wonder contracted with Northwest Sound to build a set of PA speakers of extraordinary capability -- response nearly flat out to 45 kHz, etc. . . . .
> Finally, during one show, one of the sound guys was examining the audio spectrum analyzer screen, and mistakenly pushed the 20 kHz - 200 kHz range button instead of the 2 kHz - 20 kHz button. Imagine his alarm at the sight of a potent 28 kHz component, the product of all the synthesizers' DAC update clocks. . . . .

If the DAC clock rate was 28 KHz, the synthesizers' Nyquist frequency (the highest frequency that could be reproduced) would have been only 14 KHz, which is pretty crummy and wouldn't have required a fancy sound system.

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

Ear-itation

<JOHNSON%FOR3083.ISSC@ISEC-OA.ARPA>
Tue, 18 Oct 88 17:56:23 EST

FROM: KEN JOHNSON GRC, ROOM D253 EXT.233
Subject: Ear-itation

A few years back , some pseudoscientists expressed a concern that the "anapestic" beat was so counter to the natural beat of the heart that the hearer's health and proper heart-functioning could be threatened by hearing this beat. In other words, when the thumping "We Are the Champions" anapestic (and irritating) beat is heard at sporting events, there is a major health risk! Bah, I say!

Concerning the 28K Hz problem - aren't we continually bombarding animals with much higher hearing ranges (dogs, birds(?), bats) with sounds in the post-20K Hz range? And does Stevie Wonder, with a higher dependence on his sense of hearing, notice the irritating noises more than the person with normal senses?

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 67

Tuesday 25 October 1988

Contents

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

Unplugged Cable Plugs Orlando Traffic

Scot E Wilcoxon <sewilco@datapg.MN.ORG>
Mon, 24 Oct 88 15:05:47 CDT

In the story below, it is interesting to note the mayoral aide emphasizes that the computer "system" did not fail. Apparently the operating procedures failed, and for only six minutes.

October 11th: "Computer snafu creates traffic jam"

ORLANDO, Fla. (UPI) _ An engineer's mistake paralyzed downtown traffic for six

minutes when signals remained red during lunch hour and forced the city to call out police on horseback to unclog intersections.

Traffic engineers replacing a piece of Orlando's sophisticated traffic light synchronizing system Tuesday forgot to plug in a cable, freezing the signals at 34 intersections, mostly along Orlando's busy north-south thoroughfares just after 12:30 p.m.

"It wasn't a glitch in the system. It was during an installation, someone forgot to plug in a couple of machines," said mayoral aide Joe Mittiga.

Orlando's $3 million synchronizing computer started working this summer, but Mittiga said workers adding equipment forgot to connect two parts and a backup system failed to initiate when the main computer system failed.

"They were left unplugged inadvertently for six minutes," he said.

Thousand of drivers were stuck in traffic as the lights remained on red, green or yellow, Mittiga said.

--

Scot E. Wilcoxon sewilco@DataPg.MN.ORG {amdahl|hpda}!bungia!datapg!sewilco
Data Progress UNIX masts & rigging +1 612-825-2607

Airbus A320 in service

<attcan!utzoo!henry@uunet.UU.NET>
Tue, 25 Oct 88 00:55:22 EDT

The 3 Sept issue of Flight International has a feature article about early operational experience with the A320. Apparently everyone has been rather surprised that many of its teething problems have little to do with the electronics. Spare parts, in particular, have been somewhat of a problem.

One thing the airlines are quite happy with is the Centralized Fault Display System, which keeps a running log of all in-flight problems for scrutiny by the maintenance crews. Both British Airways and Air France plan to link the CFDS to a communications system, so that faults can be reported from the air and spare parts can be waiting when the aircraft lands. At present, the written engineering log is still the official and legal record of in-flight problems, but after some more experience with CFDS this may be reconsidered. There are still occasional bugs in the CFDS software, but things are getting fixed. The airlines say that CFDS has been a major factor in keeping a new airliner running unusually well.

The fly-by-wire flight controls have behaved perfectly.

The engine-control computers likewise have a flawless record, although at one point Air France replaced a number of them due to what seems to have been a misunderstanding about the location of some problems.

Power spikes caused by the cutover from ground to onboard power have been a headache, as they tend to trigger bad-power-supply detectors in the computers. These problems invariably happen on the ground, not in flight. Work is underway on fixing them. Many of the computers affected are in very minor control roles; a particular trouble spot has been the microcomputer-controlled vacuum toilets chosen by Air France.

The biggest problem for both airlines is a set of design and manufacturing flaws in the air-conditioning units, combined with shortage of spares. Computers are not involved in this one.

Both airlines have a low opinion of the software in the Cabin Intercommunication Data System, which controls cabin lights, signs, speakers, and entertainment. Both agree that the idea of the system is good and want to see it operational, but the suppliers simply did not have production-quality software ready in time. "A kid could have written the software for the CIDS", says BA, but in fact the current [3 Sept] software simply does not work and BA has been bypassing it almost entirely. The main problem is frequent intermittent manlfunctions.

Spare flight computers are still being carried on each flight, but this is routine for major no-go items on new airliners. Airbus says that there is now enough experience to justify dispatching an A320 with one of its seven flight-control computers dead; the original rule required all to be functioning. Airbus is still working on "tidying up" the flight-control software's responses to situations where the aircraft has gone outside the normal flight envelope involuntarily, e.g. from collision damage or sudden severe turbulence. Assorted "nice to have" features are also being implemented now that the schedule pressure has relaxed.

The only change in Air France operating procedures since the airshow crash has been a firm policy that airshow appearances will not carry passengers henceforth. The wreckage is being studied for lessons to be learned; the Flight article observes that a crash into a mature forest killed only three out of 136 people. Of note are signs that the floor-level emergency lighting system may not have turned on properly, and the failure of the hand-held megaphone's mounting bracket at rather less than its rated 9G.

The 24 Sept issue reports that the pilot of the airshow crash has been fired, with the copilot's status yet to be decided. A recent report by the French civil aviation authorities contains the first independent confirmation that the accident was caused by pilot error. (The pilots' union, of course, contests this.) The report recommends an eight-year suspension of the pilot's licence, and a two-month licence suspension for the copilot.

"Officials familiar with the flight recorder evidence say that despite the pilots' assertion that the aircraft was slow in responding to the controls, the flight control computers probably prevented a worse disaster by keeping the aeroplane unstalled when the pilots realized too late that they were about to crash."

Henry Spencer at U of Toronto Zoology
uunet!attcan!utzoo!henry henry@zoo.toronto.edu

Computer Literacy

Ronni Rosenberg <ronni@VX.LCS.MIT.EDU>
Tue, 25 Oct 88 10:36:36 edt

I am writing a Ph.D. thesis on computer-literacy education. One way in which this work differs from previous work is that it incorporates the perspectives of not only educators, but also computer professionals, the most computer-literate group in society. (To the extent that "computer literacy" means anything, it must apply to computer professionals.) To get more feedback from the computer community, I am starting a RISKS dialogue on computer literacy.

I will be sending several messages about computer literacy, asking for your opinions and reactions. This is not a right-or-wrong issue. Since I am interested in what people think about computer literacy, all responses are valid! Reply to me directly if you don't think your message is appropriate for RISKS. (For instance, for my purposes, it is fine for lots of people to send messages just saying they agree with what someone else said, but such messages are best sent directly to me.) As usual, PGN will publish in RISKS the most relevant submissions. In this case, he will also forward to me the other submissions on this topic.

All submissions are confidential. Anything that I quote or paraphrase will be presented anonomously, unless I get explicit permission from an individual to use his or her name. Usually I don't attribute a comment more specifically than to say, for instance, it is from "a Computer Science professor." You can indicate in your message the sort of work you do with computers, if you like.

* * * *

In a 1985 school survey, 96% of the respondents -- classroom teachers, computer coordinators, and administrators -- said that their schools offered instruction in computer literacy. What do you know about course content and materials, school hardware and software, teacher training, and so on? Are your children learning about computers in schools? Have you been involved in any sort of school advisory committee for computer education? If computer-literacy education has not crossed your path, what do you guess is taught in a typical class?

Belgian PM's email tapped

Rodney Hoffman <Hoffman.es@Xerox.COM>
23 Oct 88 18:13:40 PDT (Sunday)

From the 'Los Angeles Times', Saturday, October 22, 1988:

BELGIAN LEADER'S MAIL REPORTEDLY READ BY HACKER

BRUSSELS (AP) -- Belgian Prime Minister Wilfried Martens on Friday ordered an investigation into reports that a computer hacker rummaged through his electronic files and those of other Cabinet members.

The newspaper De Standaard reported that a man, using a personal computer, for three months viewed Martens' electronic mail and other items, including classified information about the killing of a British soldier by the Irish Republican Army in Ostend in August.

The newspaper said the man showed one of its reporters this week how he broke into the computer, using Martens' password code of nine letters, ciphers and punctuation marks. "What is more, during the demonstration, he ran into another 'burglar' ... with whom he briefly conversed" via computer, the newspaper said.

Police find hacker...and release him

Henry Cox <cox@spock.ee.mcgill.ca>
Mon, 24 Oct 88 09:19:44 edt

[From the Montreal Gazette, 24 October, 1988]

POLICE FIND HACKER WHO BROKE INTO 200 COMPUTERS

London (New York Times) - Police said yesterday that they had found and questioned a 23-year-old man who used computer networks to break into more than 200 military, corporate, and university systems in Europe and the United States during the past five years.

The man was asked about an alleged attempt to blackmail a computer manufacturer, but an official for Scotland Yard said that there was not enough evidence to pursue the matter. He was released.

The man, Edward Austin Singh, who is unemployed, reportedly told the police he had been in contact with other computer ``hackers'' in the United States and West Germany who use communications networks to penetrate the security protecting computers at military installations.

Singh's motive was simply to prove that it was possible to break into the military systems, police said, and apparently he did not attempt espionage.

London police began an investigation after the man approached a computer manufacturer. He allegedly asked the company for $5250 in exchange for telling it how he had entered its computer network.

The company paid nothing, and London police tracked the suspect by monitoring his phone calls after the firm had told Scotland Yard about the incident.

Henry Cox (cox@spock.ee.mcgill.ca)

Aegis user interface changes planned

<jon@june.cs.washington.edu>
Mon, 24 Oct 88 09:43:56 PDT

Here are excerpts from, "Fixes to Aegis system recommended by Navy,"
by John A. Adam, THE INSTITUTE (News supplement to IEEE SPECTRUM) vol 12
no 11, Nov. 1988, pps. 1,2:

"The Chief of Naval Operations is to assess a redesign of the Aegis
large-screen display that would allow the option of showing an aircraft's
altitude directly. Admiral William J. Crowe said "it was never adequately
reconciled" why the operator misinterpreted the digital readout of the
airliner's altitude as descending while the replayed data showed constant
ascent. The descending profile added to the perception of the approaching
aircraft as hostile (in the July 3 1988 shootdown of an Iranian commercial
airliner, which was mistaken for a hostile F-14).

Four screens, which make up the principal visual information source for the
ship's top combat officers, at present show two-dimensional tracks of
targets each tagged with a 24 character alphanumeric label indicating such
data as velocity and identification ... Defense secretary Frank Carlucci
said that to find range and altitude information of a target on the screen,
one must examine a computer readout, which is distracting. "We think it's a
good idea to display altitude and range on a large screen," Carlucci said.
"I think you could probably even put an arrow on whether it's ascending or
descending." ...

The investigation also found that Iranian Flight 655 was emitting the
civilian identification-friend-or-foe (IFF) mode 3 squawk - not a military
code as had been supposed by the Vincennes crew. .. Misidentification of
the airliner's signal for a mode 2 military squawk happened because the
radar operator left his range gate at the airport for 90 seconds instead
of moving it, said Carlucci. The signal from another aircraft was picked
up, which led the Vincennes Combat Information Center to declare the contact
an F-14 fighter. ...

At the press conference, Carlucci said of the Aegis: "I'm not indicating
it wasn't designed correctly," he said, but "as you go through experience
with any weapon system you improve the design," particularly in combat.

- Jonathan Jacky, University of Washington

Programmable Hotel Locks

John Rushby <RUSHBY@csl.sri.com>
Mon 17 Oct 88 17:09:58-PDT

>From cslb!joyce!ames!mailrus!tut.cis.ohio-state.edu!bloom-beacon!apple!baum Mon Oct 17 16:54:22 PDT 1988

Article 4803 of rec.travel:
Path: cslb!joyce!ames!mailrus!tut.cis.ohio-state.edu!bloom-beacon!apple!baum
>From: baum@Apple.COM (Allen J. Baum)
Newsgroups: rec.travel
Subject: Re: Programable Hotel Locks
Message-ID: <18933@apple.Apple.COM>
Date: 17 Oct 88 20:16:04 GMT
Reply-To: baum@apple.UUCP (Allen Baum)
Organization: Apple Computer, Inc.

>In article <7366@aw.sei.cmu.edu> weinstoc@sei.cmu.edu (Chuck Weinstock) writes:
>I wasn't sure where to post this, but rec.travel seems like a
>reasonable possibility. Many hotels these days have programmable
>locks. Upon checkin, a card is either magnetized or punched and
>serves as your key. My question is, how is the lock itself
>programmed? It's hard to believe that they run wires all around the
>hotel and through the hinge of the door, though I suppose that's possible.
>
>Chuck Weinstock

I've been told that the locks contain a feedback-shift-register, or
something similar. It, internally, generates the next key. If a key
it doesn't recognize is inserted, it checks it against the next key.
If it matches, the lock advances to the next combination. At the
desk, they know how to generate a new combination from an old one,
and they know the last key issued, so they merely generate the new key.
Simply inserting the new, valid key into the lock does all the work of
updating. Presumably, there are also master-key, and resetting provisions.

what th

--
{decwrl,hplabs}!nsc!baum@apple.com (408)973-3385

Nausea-inducing frequencies (Re: RISKS-7.66)

David Chase <chase@orc.olivetti.com>
Thu, 20 Oct 88 16:45:34 -0700

Ask any competent neurologist and you should get a quick answer. Flashing
lights at certain frequencies (I think 15Hz is one very important one) can
induce nausea and/or epileptic seizures in some people. A neurologist told
me of encountering three people in one day who had been zarked by the same
failing flourescent bulb at a meat counter. Flashing lights are also a part
of EEGs taken when epilepsy is suspected.

As far as the props go, it could have been a visual flicker effect, or it
could be that sounds can have a similar effect. May I suggest (to the
curious among the audience) that you NOT try this experiment at home;
epileptic seizures are not especially good for you, and the known occurrence
of one tends to legally hinder your use of heavy equipment (like
automobiles) for a period of time.

David

Risks in Foundations of Numerical Analysis

John Cherniavsky <jcc@mimsy.umd.edu>
Fri, 21 Oct 88 10:28:43 EDT

In the October 1988 Bulletin of the American Mathematical Society there is an article by Peter Linz, "A Critique of Numerical Analysis", that points up the inadequacy of the foundations of numerical analysis. In that article he points out the inadequacies of current error analysis, the lack of information regarding the fit of the numerical model to the real world phenomenon that is being modeled (inappropriate choice of norm is his example), and the lack of a mechanism to validate or test the numerical model against the real world phenomenon being modeled.

With the advent of computers that can carry out three dimensional numerical modeling and the use of such computers in the design of safety critical systems (such as airplanes), a lack of adequate mathematical foundations for numerical analysis could lead to serious consequences.

Takeoff warning systems to be tested

Henry Cox <cox@spock.ee.mcgill.ca>
Fri, 21 Oct 88 11:18:41 edt

[From the Montreal Gazette, 21 October, 1988

JET TAKEOFF WANING SYSTEMS TO BE TESTED

Washington (AP) - The government has ordered immediate tests of takeoff alarm systems on nearly 1800 Boeing 727 and Boeing 737 jetliners in the U.S. after finding "a significant number" of the alarms not working properly.

The alarms are a critical safety device because they warn pilots if they have improperly set imstruments or control devices during takeoff.

The Federal Aviation Authority yesterday told the U.S. airlines they must conduct the tests immediately and continue the checks every 200 flight hours.

Last year, the failure of pilots to set their flaps properly led to the crash of a Northwest Airlines jet in Detroit, killing 156 people.

Investigators say a similar oversight remains a possibility in the crash of a Delta Air Lines Boeing 727 in Detroit last August in which 14 people were killed.

In neither case was there any evidence that the takeoff alarm sounded.

The Delta crash led the aviation authority to order airlines in September to check the alarm systems on nearly 1200 Boeing 727 aircraft.

The agency said yesterday tose checks resulted in "a significant number of inoperative warning systems discovered" on the Boeing 727 aircraft. It said that in 35 cases, the warning alarm either failed altogether or operated improperly.

Although the September tests covered only Boeing 727s, the agency concluded all Boeing 737 aircraft because their alarm systems are "similar...and subject to similar fairlures."

[Of course, even if the alarms do work properly, they must be ON to be effective. In the wake of the crashes in India on 19 October, there have been several stories in the paper about other crashes where the pilot turned off the alarms because they were annoying him, and then neglected to put the landing gear down.]

Henry Cox

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 68

Monday 31 October 1988

Contents

- Conspiracy to Defraud
  - Martyn Thomas
- `Runaway' Computer Projects
  - Rodney Hoffman
- Perceived risk
  - James F. Carter
- "TCA pushes for privacy on corporate networks"
  - Jerry Leichter
- Risks in Answering Machines
  - Andy Glew
- Ear-itation
  - Ed Ravin
- Info on RISKS (comp.risks)

Conspiracy to Defraud

Martyn Thomas <mct@praxis.UUCP>
Wed, 26 Oct 88 15:04:46 BST

The Confederation of British Industry has submitted a proposal to the Law Commission proposing changes to the law on conspiracy to defraud.

They propose (inter alia) that current offences involving "deception" (which require that a human mind is deceived) should be extended to include deception of machines, including (in particular) computers.

This sounds risky - can anyone think of good examples of unintended consequences?

Martyn Thomas !uunet!mcvax!ukc!praxis!mct

`Runaway' Computer Projects

Rodney Hoffman <Hoffman.es@Xerox.COM>
30 Oct 88 13:20:56 PST (Sunday)

In the November 7, 1988 issue, 'Business Week' has a two-page story headlined "IT'S LATE, COSTLY, INCOMPETENT -- BUT TRY FIRING A COMPUTER SYSTEM: Companies get stuck with 'runaways' that trample all over their budgets and reputations." Nothing amazingly new, but a good summary of the problems, with several case histories.

From the article: "A recent Peat Marwick Mitchell & Co. survey of 600 of the accounting firm's largest clients highlighted the problem: Some 35% currently have major runaways.... In 1986, [a management consultant] set up a group at Peat Marwick to rein in runaways. Since then, he has had $30 million in revenues from nearly 20 clients...."

Two sidebars are of interest:

A SAMPLING OF `RUNAWAY' PROJECTS

* ALLSTATE INSURANCE. In 1982, with software from Electronic Data Systems, the insurer began to build an $8 million computer system that would automate it from top to bottom. Completion date: 1987. An assortment of problems developed, delaying completion until 1993. The new estimated price: $100 million.
* CITY OF RICHMOND. In 1984 it hired Arthur Young to develop a $1.2 million billing and information sytem for its water and gas utilities. Completion date: March, 1987. After paying out close to $1 million, Richmond recently canceled the contract, saying no system had been delivered. Arthur Young has filed a $2 million breach of contract suit against the city.
* BUSINESS MEN'S ASSURANCE. In 1985 the reinsurer began a one-year project to build a $500,000 system to help minimize the risk of buying insurance policies held by major insurers. The company has spent nearly $2 million to date on the project, which is in disarray. The new completion date is early 1990.
* STATE OF OKLAHOMA. In 1983 it hired a Big Eight accounting firm to design a $500,000 system to handle explosive growth in workers' compensation claims. Two years and more than $2 million later, the system still didn't exist. It finally was finished last year at a price of nearly $4 million.
* BLUE CROSS AND BLUE SHIELD UNITED OF WISCONSIN. In late 1983 it hired Electronic Data Systems to build a $200 million computer sytem. It was ready 18 months later -- on time. But it didn't work. The system spewed out some $60 million in overpayments and duplicate checks before it was harnessed last year. By then, Blue Cross says, it had lost 35,000 policyholders.

[Several of these are discussed in more detail in the article.]

HOW TO KEEP A PROJECT UNDER CONTROL

* Before designing the system, get suggestions from the people

who will use it.
* Put senior, nontechnical management in charge of the project to help ensure that it is finished on time and within budget
* Set up 12-month milestones -- interim deadlines for various parts of the project
* Insist on performance clauses that hold suppliers legally responsible for meeting deadlines
* Don't try to update the system in midstream, before the original plan is finished

---

Perceived risk

<jimc@math.ucla.edu>
Wed, 26 Oct 88 16:22:19 PDT

Freudenburg, William R, "Perceived Risk, Real Risk: Social Science and the Art of Probabilistic Risk Assessment", Science, vol 242 #4875 (10/7/88) p.44. A very interesting article. The author's thesis is that risks computed from "hard scientific evidence" frequently inadequately predict both the probability and the consequences of a risk, because human factors are inadequately modelled. Risk estimation workers suffer from non-obvious human errors. The general public are not as irrational as they sometimes seem to technical people, when their concerns, values and experience history are taken into account.

Readers of this newsgroup may already "know" all this, but it's useful to have our noses rubbed in it yet again.

James F. Carter (213) 825-2897
UCLA-Mathnet; 6608B MSA; 405 Hilgard Ave.; Los Angeles, CA 90024-1555

"TCA pushes for privacy on corporate networks"

LEICHTER-JERRY@CS.YALE.EDU <"Jerry Leichter>
Wed, 19 Oct 88 14:54 EST

[Entered without permission from Computerworld, 3 Oct 88, page 133]

By Kathy Chin Leong, CW Staff

SAN DIEGO --- As more and more confidential data winds its way across computer networks, users are expressing alarm over how much of that information is safe from subsidiaries of the Bell operating companies and long-distance firms providing transmission services.

This fear has prompted the Tele-Communications Association (TCA) and large network users to appeal to the Federal Communications Commission to clarify exactly what network data is available to these vendors.

Users with large networks, such as banks and insurance companies, are concerned that published details even of where a circuit is routed can be

misused. "We don't what someone like AT&T to use our information and then turn around and compete against us," said Leland Fong, a network planner at Visa International in San Francisco. Users are demanding that the FCC establish a set of rules and regulations so that information is not abused.

At issue is the term "customer proprietary network information" (CPNI), which encompasses packet data, address and circuit information and traffic statistics on networks. Under the FCC's Computer Inquiry III rules, long-distance carriers and Bell operating companies --- specifically, marketing personnel --- can get access to their own customers' CPNI unless users request confidentiality. What his group wants, TCA President Jerry Appleby said, is the FCC to clarify exactly what falls under the category of CPNI.

Fong added that users can be at the mercy of the Bell operating companies and long-distance vendors if there are no safeguards established. Customer information such as calling patterns can be used by the operating companies for thier own competitive advantage. "At this time, there are no controls over CPNI, and the users need to see some action on this," Fong said.

SPREAD THE CONCERN

At a meeting here during the TCA show, TCA officials and the association's government liason committee met with AT&T to discuss the issue; the group will also voice its concerns to other vendors.

Appleby said the issue should not be of concern just to network managers but to the entire company. Earlier this month, several banks, including Chase Manhattan Bank and Security Pacific National Bank, and credit card companies met with the FCC to urge it to come up with a standard definition for CPNI, Appleby said.

While the customer information is generally confidential, it is available to the transmission carrier that is supplying the line. The data is also available to marketing departments of that vendor unless a company asks for confidentiality. Fong said that there is no regulation that prevents a company from passing the data along to its subsidiaries.

[Comment: What I find particularly fascinating about this article is its perfect illustration of the world-view of large businesses. Banks, insurance companies and credit agencies collect tons of information about individuals, which they then wish to treat as their private property, to do with as they see fit. They fight "government interference" intended to protect the privacy of that data as expensive, burdensome and unnecessary.

But when their precious data is moved over AT&T's lines, all of a sudden they are very concerned that AT&T not abuse it. Not only that, but they want the government to make SURE that AT&T remains on its best behavior!

-- Jerry]

Risks in Answering Machines (revisited)

Andy-Krazy-Glew <aglew%vger@xenurus.gould.com>
Tue, 25 Oct 88 20:12:54 CDT

Recently I went to purchase an answering machine. Modern answering machines have all sorts of remote features, features that can be exercised from another phone, by generating touch tones. These features include the ability to listen to already recorded messages, erase already recorded messages, change the outgoing message that answers the phone, etc.

There is almost no security for these remote features. The machine I bought has a two digit code, with one digit factory set, and the second digit set by a switch on the machine. The user settable digit can only be set to 3 values!

Now, I don't have many secrets, so the idea of people listening to my recorded messages doesn't bother me too much (except for the possibility that a criminal watching my house and knowing my number could intercept a message from me telling my wife that I won't be home for several hours).

But I do not like the possibility that someone could, maliciously or accidentally, erase messages, or change my answering message.

And I most emphatically do not like the remote listen feature, whereby anyone can call my answering machine, press a dial tone, and listen to anything going on in my apartment.

I spent some time looking for a basic answering machine that had only the most basic remote feature, the ability to listen to recorded messages remotely, *without* having them erased. There doesn't seem to be such a system -- if you can remotely listen, you can remotely erase. Unfortunately, it does not seem possible to selectively disable these remote features.

Most salespeople were surprised by my concern, but one gave me the service numbers for Panasonic and GE. The Panasonic service was distinctly unhelpful, unable to understand why one might want more than the 256 password possibilities in their top of the line model (a model that uses 3 digits, only one of which is user settable). The Panasonic service refused even to give me an address to which I might write to describe what I think a secure answering machine should be. The GE service was much more sympathetic - but, unfortunately, GE's consumer electronics was sold to Thomson a while back, and the GE service didn't know where to forward consumer suggestions.

All this leads me to several questions:

(1) Are there any answering machines that have redefinable passwords that are long enough for an acceptable level of security?

(2) Are there any answering machines that have only non-destructive remote commands, ie. that only allow messages to be listened to remotely, not reset and overwritten?

(3) Have there been any incidents of remote sabotage of answering machines, or, worse, criminal interception of messages, or bugging, as I describe above?

Andy "Krazy" Glew, Motorola Microcomputer Division, Champaign-Urbana Development Center [lengthy trailer and disclaimer deleted. PGN]

Ear-itation

Ed Ravin <eravin@dasys1.UUCP>

24 Oct 88 15:10:19 GMT

I've got my own story to tell about high frequency noises crawling out of computer related devices, and since I'm new to RISKS, my apologies if any or all of this has been discussed before.

It all started back in college, when I went to a little office in the computing center. I walked into the room and immediately clapped my hands two my ears and shouted in aversion to the awful sound I was hearing. The two techs in the room, who worked in there most of the day, looked at me like I was crazy, because they didn't hear anything. It turned out to be the high-frequency whining from a Televideo terminal's flyback transformer. The two technicians never reported any ill effects from it. The few times I visited them again I had to stay outside of the office because of the direct pain I would experience walking in there when that terminal was turned on.

After that I began noticing the sounds made by all the other CRT's in my life. They were high pitched and slightly irritating, but not painful.
I had always, even before meeting computers, noticed the 15khz whine from a TV set, but it had never bothered me.

My next experience was with a DEC VT-100. I visited a friend of mine who had an operating VT-100 in a little room in his house. Again, I heard a loud, high pitched whine that I felt as pressure in my ears and pain. He noticed nothing, but said that that particular VT-100 was stacked with option boards and might be overloading its power supply. I've worked with other VT-100 terminals and noticed noise, but not anywhere near as bad as that sample.

And the best story of all is the AT&T Unix PC. All of the Unix PC's I ever worked with had a high-frequency noise problem to one extent or another, but the worst offenders were the ones with 40 meg disk drives installed. As soon as I turned on of them on, I would hear a high pitched noise that would slowly rise in pitch until it either went beyond my audible range or got lost in the fan noise. I thought nothing more of it until I realized that I was getting headaches, stomachaches, and feeling irritable without knowing why. I moved the machine to a closet and used it remotely. I polled everyone else at the office, as well as a few visitors from AT&T: almost noone could hear the noise from it, but anyone who had to work in the same room as the machine would eventually start complaining, even if the machine was parked in a noisy machine room. This wasn't limited to one sample, because we returned the machine and got it replaced two or three times, and none of them were acceptable to me. It wasn't just me, because we tried it out on a few other employees, who complained of irritation, stomachaches and toothaches after being in the same room as the Unix PC after a few days. This noise was definitely associated with the hard drive (as opposed to the flyback transformer who is the usual culprit), and was in the 20khz or above range, since I couldn't directly hear it, but felt it as a slight pressure in my ears.

I have walked up to airline reservation counters, car rental counters, and other service desks where the ubiquitous VDT is part of the worker's routine, where the worker must sit in front of the terminal all day, and blanched from the whine coming out of the back of the CRT. As a white collar employeee in a technical office, with a moderately eloquent speaking ability, I was able to explain to my managers why I couldn't use certain equipment and they understood

and assisted me. The information industry service worker has no such options: you can work on the machine or you can get another job. Managers over 40 probably can't even hear at 15khz, and will not understand what you're talking about. There have been numerous studies of "cluster miscarriages", where a high proportion of pregnant women using a particular brand of VDT all experience miscarriages, but most studies of VDT hazards seem to focus on low level radiation and ignore sound emissions completely.

There are no OSHA or NIOSH standards on high-frequency sound or ultrasound emmissions from devices in the workplace: the engineers who build these things are used to listening to 15 or 20 khz whines all day long and no longer notice such things. Maybe my problem is that I never listened to loud rock music and my hearing above 15khz is mostly intact. But even when you can't hear it, that noise can still bother you, as witnessed by the Stevie Wonder experience (if not my own). And I wouldn't be surprised if it has a factor in miscarriages: one of the things ultrasound can do is heat up the tissue under your skin, which is related to the hospital uses of ultrasound devices. The scary thing is that so many people just dismiss this problem because they "can't hear it".

Ed Ravin | cucard!dasys1!eravin
(BigElectricCatPublicUNIX)| eravin@dasys1.UUCP
Reader bears responsibility for all opinions expressed in this article.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 69

Thursday 3 November 1988

Contents

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

Virus on the Arpanet - Milnet

<Stoll@DOCKMASTER.ARPA>
Thu, 3 Nov 88 06:46 EST

Re Arpanet "Sendmail" Virus attack November 3, 1988

Hi Gang!

It's now 3:45 AM on Wednesday 3 November 1988. I'm tired, so don't believe everything that follows...

Apparently, there is a massive attack on Unix systems going on right now.

I have spoken to systems managers at several computers, on both the east & west coast, and I suspect this may be a system wide problem.

Symptom: hundreds or thousands of jobs start running on a Unix system bringing response to zero.

Systems attacked: Unix systems, 4.3BSD unix & variants (eg: SUNs) any sendmail compiled with debug has this problem. See below.

This virus is spreading very quickly over the Milnet. Within the past 4 hours, I have evidence that it has hit >10 sites across the country, both Arpanet and Milnet sites. I suspect that well over 50 sites have been hit. Most of these are "major" sites and gateways.

Method:

Apparently, someone has written a program that uses a hole in SMTP Sendmail utility. This utility can send a message into another program.

Step 1: from a distant Milnet host, a message is sent to Sendmail
to fire up SED, (SED is an editor) This is possible in certain
versions of sendmail (see below).

2: A 99 line C program is sent to SED through Sendmail.

3: The distant computer sends a command to compile this C program.

4: Several object files are copied into the Unix computer.
There are 3 files: one targeted to Sun
one targeted to SUN-3
one targeted to vax (ultrix probably, not vms)

5: The C program accepts as address other Milnet sites

6: Apparently, program scans for other Milnet/arpanet addresses and
repeats this process.

The bug in Sendmail:

When the Unix 4.3 BSD version of Sendmail is compiled with the Debug option, there's a hole in it.

Most Unix systems (BSD 4.3 and Suns) apparently do not have this bug. It exists only where the system manager recompiled Sendmail and enabled debugging.

This is bad news.

Cliff Stoll dockmaster.arpa

More on the virus

Gene Spafford <spaf@purdue.edu>
Thu, 03 Nov 88 09:52:18 EST

All of our Vaxen and some of our Suns here were infected with the virus. The virus forks repeated copies of itself as it tries to spread itself, and the load averages on the infected machines skyrocketed. In fact, it got to the point that some of the machines ran out of swap space and kernel table entries, preventing login to even see what was going on!

The virus seems to consist of two parts. I managed to grab the source code for one part, but not the main component (the virus cleans up after itself so as not to leave evidence). The way that it works is as follows:

1) Virus running on an infected machine opens a TCP connection to a victim machine's sendmail, invokes debug mode, and gets a shell.

2) The shell creates a file in /tmp named $$,l1.c (where the $$ gets replaced

by the current process id) and copies code for a "listener" or "helper" program. This is just a few dozen lines long and fairly generic code. The shell compiles this helper using the "cc" command local to the system.

3) The helper is invoked with arguments pointing back at the infecting virus (giving hostid/socket/passwords as arguments).

4) The helper then connects to the "server" and copies a number of files (presumably to /tmp). After the files are copied, it exec's a shell with standard input coming from the infecting virus program on the other end of the socket.

From here, I speculate on what happens since I can't find the source to this part lying around on our machines:

5) The newly exec'd shell attempts to compile itself from the files copied over to the target machine. I'm not sure what else the virus does, if anything -- it may also be attempting to add a bogus passwd file entry or do something to the file system. The helper program has an array of 20 filenames for the "helper" to copy over, so there is room to spare. There are two versions copied -- a version for Vax BSD and a version for SunOS; the appropriate one is compiled.

6) The new virus is dispatched. This virus opens all the virus source files, then unlinks the files so they can't be found (since it has them open, however, it can still access the contents). Next, the virus steps through the hosts file (on the Sun, it uses YP to step through the distributed hosts file) trying to connect to other machines' sendmail. If a connection succeeds, it forks a child process to infect it, while the parent continues to attempt infection of other machines.

7) The child requests and initializes a new socket, then builds and invokes a listener with the new socket number and hostid as arguments (#1, above).

The heavy load we see is the result of multiple viruses coming in from multiple sites. Since local hosts files tend to have entries for other local hosts, the virus tends to infect local machines multiple times -- in some senses this is lucky since it helps prevent the spread of the virus as the local machines slow

down.

The virus also "cleans" up after itself. If you reboot an infected machine (or it crashes), the /tmp directory is normally cleaned up on reboot. The other incriminating files were already deleted by the virus itself.

Clever, nasty, and definitely anti-social.

--spaf

More on the virus attack

Peter Neumann <neumann@csl.sri.com>
Thu, 3 Nov 1988 14:27:22 PDT

Remember that the above are preliminary messages relating to an event in progress. There seem to be many unanswered questions. Perhaps someone will contribute a definitive report to the next issue of RISKS.

Examination of the code suggests a fairly sophisticated person writing relatively high quality (although undocumented) code, exploiting several flaws that exist(ed) on many UNIX systems, and written with considerable good practice in self-checking, reliability, etc. From the evidence thus far, I would guess it that this was a deliberate attack, not an accidental experiment run astray.

Although it was primarily a denial of service attack, it did some remarkable things, taking advantage of many different approaches. The spawned processes appear to have been doing attacks on encrypted passwords to enable ftps (in case the .rhost attack would not work -- cf. the Stanford breakins described in CACM and SEN by Brian Reid). Separate versions to run on Suns and Vaxens were apparently propagated in DES encrypted form, decrypted, and both programs tried to see which one would work.

We quoted Henry Petroski here over a year ago to the effect that we do not learn from our successes, but that we have an opportunity to learn from our failures. Once again we are presented with the opportunity to learn that many of our computer systems have serious security vulnerabilities, and that we need to take pains to defend against the really malicious attacks. Strangely some people take heart in the fact that the security attacks to date (whether penetrations, exploitations of privilege, Trojan horses, or legitimate viruses) have been relatively modest in scale, perhaps to justify the absence of concern. I am afraid that it will take a Chernobyl- or Three-Mile-Island-like disaster before the community at large wakes up. PGN

More on the virus

Matt Bishop <bishop@bear.Dartmouth.EDU>
Thu, 3 Nov 88 16:32:25 EST

... This program introduced itself through a bug in sendmail. At these sites,

sendmail was compiled and installed with a debugging option turned on. As near as I can figure (I don't have access to the sendmail sources), by giving a specific option to the "debug" command in sendmail (there are lots of those, controlling what exactly you get information about) you can cause it to execute a command. As sendmail runs setuid to root, guess what privileges the command is executed with. Right.

Apparently what the attacker did was this: he or she connected to sendmail (ie, telnet victim.machine 25), issued the appropriate debug command, and had a small C program compiled. (We have it. Big deal.) This program took as an argument a host number, and copied two programs -- one ending in q.vax.o and the other ending in .sun.o -- and tried to load and execute them. In those cases where the load and execution succeeded, the worm did two things (at least): spawn a lot of shells that did nothing but clog the process table and burn CPU cycles; look in two places -- the password file and the internet services file -- for other sites it could connect to (this is hearsay, but I don't doubt it for a minute.) It used both individual .rhost files (which it found using the password file), and any other remote hosts it could locate which it had a chance of connecting to. It may have done more; one of our machines had a changed superuser password, but because of other factors we're not sure this worm did it.

This last part is still sketchy; I have the relevant sun.o file and will take it apart to see just what it was supposed to do. As of now, it appears there was no serious damage (just wasted CPU cycles and system administrator time).

Two obvious points:

1. Whoever did this picked only on suns and vaxen. One site with a lot of IRISes and two Crays (ie, NASA Ames) got bit on their Suns and Vaxen, but the attempt to get the other machines didn't work.
2. This shows the sorry state of software and security in the UNIX world. People should NEVER put a program with debugging hooks in it, especially when the hook is (or can be made) to execute an arbitrary command. But that is how the sendmail which was used was distributed!

One more interesting point: initially, I thought an application of the "principle of least privilege" would have prevented this penetration. But the attacker used a world-writeable directory to squirrel the relevant programs in, so -- in effect -- everything could have been done by any user on the system! (Except the superuser password change, of course -- if this worm did in fact do it.)

I think the only way to prevent such an attack would have been to turn off the deug option on sendmail; then the penetration would fail. It goes to show that if the computer is not secure (and like you, I don't believe there ever will be such a beastie), there is simply no way to prevent a virus (or, in this case, a worm) from getting into that system.

I know this is somewhat sketchy, flabby, and fuzzy, but it's all I know so far. I'll keep you posted on developments ...

Matt

A320 update

Steve Philipson <steve@aurora.arc.nasa.gov>
Mon, 31 Oct 88 11:39:11 PST

Henry Spencer's recent article on the A320's first six months in service states that the fly-by-wire system has "behaved perfectly." It should be noted, however, that the article he was referring to clearly pointed out that there were failures of the primary flight guidance computer, which were rectified by backup systems.

More information from Flight:

From Flight International, 9/24/88:

"Five months after entry into commercial service with Air France, British Airways, and Air Inter, Airbus Industries' A320 fly-by-wire 150-seat airliner still has many teething problems, but fewer than other European or American transport aircraft in their first year, say the manufacturers and operators [Note: Air France and BA have been running rather old fleets for a LONG time]

"Air France's Airbus A320 Ville de Paris, on flight AF914 from Paris to Amsterdam on August 26, had to turn back shortly after takeoff from Charles de Gaulle with 81 passengers on board. A series of warnings included a toilet fire indication, which subsequently proved to be a false alarm.

"When the pilot attempted to land the aircraft, yet another warning light erroneously indicated that the landing gear was not down. The A320 made a pass over the airport, and the control tower confirmed that the landing gear was down. A second pass was then made, and Air France ground engineers andmechanics confirmed that the gear was down. The pilot made a perfect landing, although the computer display system displayed many false warnings.

"Passengers on the A320, which had taken off 40 min. late because of heavy traffic, had to transfer to two other aircraft, causing a 4 hr delay.

"The faulty A320 was grounded for two days pending thorough checks, but is now back in regular service to Dusseldorf, Amsterdam, and Geneva.

"Earlier, on August 19, an Airbus A320 belonging to French domestic carrier Air Inter reported a double power failure on a flight from Nice Cote d'Azur to Paris. According to a computer system warning, the auxilliar power unit broke down at the same time as one of the two main generators, a little while before landing at Orly airport. The pilot made a safe landing, as his aircraft still had three additional power sources--the second main generors, batteries, and the other auxilliary power unit.

"On March 28, Air France's Ville de Paris had encountered similar problems on its inaugural flight over Paris and the Champs Elysees with then Prime Minister Jacques Chirac and 150 other passengers.

"Since entry into commercial service, only three per cent of A320 flights have been delayed beyond the accepted 15 min. by technical problems, says Airbus Industrie technical vice-president Bernard Ziegler. 'This 97 per cent rate of technical regularity is very close to the best aircraft in service, which have attained 98 per cent or 98.3 per cent,' he says. "For a brand new aircraft with revolutionary avionics and fly-by-wire, the A320 hasmade a remarkable achievement.'

The loss of Air France's third A320, Ville d'Amsterdam, at Mulhouse Habsheim airport during a local aero club rally on June 26, with three dead and 50 injured among its 153 joyriding passengers, has caused great concern, although the aircraft has been cleared of any malfunction and the accident was attributed to pilot error. Air Inter's pilots' union added to the general concern by striking in protest against the A320's two-man crew [but largely on the basis of pay and seniority, with safety as a propaganda gimmick].

'Every day in Europe, five airliners on average turn back for various technical reasons,' says Bernard Ziegler. 'That does not make news. But when the A320 is one of the five, then the mass media cries out. That's the rule of the game. But we are satisfied the A320 is all right--nothing wrong with it. It's a very good plane.'

Any new aircraft undergoes a series of technical adjustments in its first months of operation, he notes. 'It took Boeing two-and-a-half years for the 757, a year for Airbus Industrie with the A300, and hopefully it will only take us nine months for the A320,' says Ziegler."

I find Ziegler's rationale for the failures of the A320 somewhat disturbing. With only a handful of airplanes in service, for any significant percentage of in-flight or on-ground failures to occur, and then say it should be compared to the massive fleets of existing aircraft, is to obfuscate the issue.

His confidence in the A320's backup electrical systems is also rather odd, considering the airplane's susceptibility to transient controls, and his company's failure to provide even a mediocre cabin lighting control system.

Re: Conspiracy to Defraud

<dan@WILMA.BBN.COM>
Tue, 01 Nov 88 16:39:47 -0500

Re the Confederation of British Industry's proposal to change the law on defrauding to include deception of computers as well as people:

To state the obvious, computer programs are so limited in their ability to understand what someone might be trying to do, and what information is

necessary for that purpose, that it's often necessary to "deceive" them just to get them to do the right thing. It's much like the problem of figuring out what to put on a complex form, like tax forms: every individual situation is different, and the form either provides no way at all to say what your situation is, or provides several equally plausible ways to express it. But at least forms have margins, and you can attach additional pieces of paper to them. Computer-based "forms" have neither.

Here's an example: in the process of trying to provide some service, a computer asks for my telephone number. I don't believe it has any right to that number for this purpose, so I refuse to answer. But it won't go on to the next query until I answer that one. I find someone in charge: "I don't want to give my phone number out. Is that OK?" "Sure. Just give it a fake number and go on." The computer is now "deceived". It's ridiculous to think that both I and the computer's owner could now be charged with fraud!

Taken literally, such a law would also preclude thorough testing of computer software. In testing, you're almost always "deceiving" the computer in order to see whether it will handle some case correctly, particularly if you're checking error handling. Are testers going to have to insert special routines that print out "It's OK, I know this is a test" before giving any answers, to avoid prosecution?

There are also serious theoretical problems with the notion of "deceiving" a computer. In theory, deception occurs when an individual is deliberately led to believe X when not-X is true. But what does "belief" mean when applied to a computer system? If I have a file on a computer system that says I'm 3 years old, does that mean the computer "believes" I'm three years old? Of course not, you say. What if it's in a database? Is it deception then?

I think it's all the fault of some AI people who would like us to think that all it takes to be able to say that a computer system believes a fact is that it's in a Lisp-based inference system that includes a "believes" predicate!

Dan Franklin

Re: Telephone answering machines

Vince Manis <manis@grads.cs.ubc.ca>
Tue, 1 Nov 88 16:30:36 PST

I was concerned about security when I bought a new answering machine this spring. I finally settled on a GE model which has an 8-bit security code (which you set in octal!), believing that a search space of 256 is large enough. (There--all you have to do is look me up in the phone book and you have enough information to crack my code. Some people are just not security-conscious enough.)

The search space seemed large enough on the following grounds:

1) there aren't many answering machine hackers around;

2) I rarely store confidential data on my machine;

3) people aren't patient enough to call a number 256 times just to break in.

Now, what I'm surprised at is that this is *exactly* the reasoning that those operating computers have used, and I knew that at the time, having read lots of papers on security. I hadn't even thought about only allowing non-destructive operations, though again this is something that anybody who has ever used anonymous ftp knows about immediately.

Am I overreacting, or is it really better to say that those who are cognisant of history are also doomed to repeat it?

Vincent Manis, Manager, Instructional Laboratories,
Department of Computer Science, University of British Columbia

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 70

Thursday 3 November 1988

Contents

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

Updated worm report

Gene Spafford <spaf@purdue.edu>
Fri, 04 Nov 88 00:27:54 EST

This is an updated description of how the worm works (note: it is technically a worm, not a virus, since it does not attach itself to other code {that we know about}):

All of our Vaxen and some of our Suns here were infected with the worm. The worm forks repeated copies of itself as it tries to spread itself, and the load averages on the infected machines skyrocketed. In fact, it got to the point that some of the machines ran out of swap space and kernel table entries, preventing login to even see what was going on!

The worm seems to consist of two parts. The way that it works is as follows:

1) Virus running on an infected machine opens a TCP connection to a victim machine's sendmail, invokes debug mode, and submits a version

of itself as a mail message.
OR it uses rsh to create itself on the remote machine through an account requiring no password (due to hosts.equiv or .rhosts entries). *OR* it gets in via a bug in fingerd *OR* it uses telnet (more on this later).

Using the sendmail route, it does something like:
From: /dev/null
To: "|sed -e 1,/^$/d | sh; exit 0"

cd /usr/tmp
cat > x14481910.c <<'EOF'

A worm "condom"

Gene Spafford <spaf@purdue.edu>
Thu, 03 Nov 88 21:20:10 EST

... Kevin Braunsdorf & Rich Kulawiec (Purdue-CC) have come up with a "condom" to protect your machine against the CURRENT worm. They are not 100% sure it works, but it seems to be completely effective and it can't do any harm. As ROOT, do:

mkdir /usr/tmp/sh
chmod 111 /usr/tmp/sh

Then edit your rc.local file to recreate the directory in case of a reboot. This will not stop a current infection, but it will prevent any new ones from taking hold -- it prevents the worm from creating replicas.

... --spaf

A cure!!!!!

Gene Spafford <spaf@purdue.edu>
Thu, 03 Nov 88 22:04:15 EST

FLASH!!

Kevin ("Adb's your friend.") Braunsdorf just burst into my office with a cure discovered in the disassembled worm binary.

If there is an external variable in the library named "pleasequit" that is non-zero, the worm will die immediately after exiting. Thus, to kill any new worms, include a patch in your library that defines the symbol. The following shell file and source code will modify your C library to define this symbol.

It WON'T kill any currently linked and running versions, but it will prevent reinfection.

Shar archive. Give the following as input to /bin/sh

```
#  Packed Thu Nov  3 21:56:35 EST 1988 by spaf@uther.cs.purdue.edu
#
#  This archive contains:
#   foo.sh
#   foo.c
#
#
echo x - foo.sh
sed 's/^X//' >foo.sh <<'*-*-END-of-foo.sh-*-*'
Xcc -c foo.c -o foo.o
Xcp /lib/libc.a /lib/libc.a.old
Xar q /lib/libc.a foo.o
Xranlib /lib/libc.a
*-*-END-of-foo.sh-*-*
echo x - foo.c
sed 's/^X//' >foo.c <<'*-*-END-of-foo.c-*-*'
Xextern int pleasequit = -1;
*-*-END-of-foo.c-*-*
exit
```

Computer Network Disrupted by `Virus'

the tty of Geoff Goodfellow <geoff@fernwood.mpk.ca.us>
Thu, 3 Nov 88 21:30:19 PST

COMPUTER NETWORK DISRUPTED BY `VIRUS'
By JOHN MARKOFF=
c.1988 N.Y. Times News Service=

In an intrusion that raises new questions about the vulnerability of the nation's computers, a nationwide Department of Defense data network has been disrupted since Wednesday night by a rapidly spreading ``virus'' software program apparently introduced by a computer science student's malicious experiment.

The program reproduced itself through the computer network, making hundreds of copies in each machine it reached, effectively clogging systems linking thousands of military, corporate and university computers around the country and preventing them from doing additional work. The virus is thought not to have destroyed any files.

By late Thursday afternoon computer security experts were calling the virus the largest assault ever on the nation's computers.

``The big issue is that a relatively benign software program can virtually bring our computing community to its knees and keep it there for some time,'' said Chuck Cole, deputy computer security manager at Lawerence Livermore Laboratory in Livermore, Calif., one of the sites affected by the intrusion. ``The cost is going to be staggering.''

Clifford Stoll,^ @a computer security expert at Harvard University, added: ``There is not one system manager who is not tearing his hair out. It's causing enormous headaches.''

The affected computers carry routine communications among military officials, researchers and corporations.

While some sensitive military data are involved, the nation's most sensitive secret information, such as that on the control of nuclear weapons, is thought not to have been touched by the virus.

Computer viruses are so named because they parallel in the computer world the behavior of biological viruses. A virus is a program, or a set of instructions to a computer, that is deliberately planted on a floppy disk meant to be used with the computer or introduced when the computer is communicating over telephone lines or data networks with other computers.

The programs can copy themselves into the computer's master software, or operating system, usually without calling any attention to themselves. From there, the program can be passed to additional computers.

Depending upon the intent of the software's creator, the program might cause a provocative but otherwise harmless message to appear on the computer's screen. Or it could systematically destroy data in the computer's memory.

The virus program was apparently the result of an experiment by a computer science graduate student trying to sneak what he thought was a harmless virus into the Arpanet computer network, which is used by universities, military contractors and the Pentagon, where the software program would remain undetected.

A man who said he was an associate of the student said in a telephone call to The New York Times that the experiment went awry because of a small programming mistake that caused the virus to multiply around the military network hundreds of times faster than had been planned.

The caller, who refused to identify himself or the programmer, said the student realized his error shortly after letting the program loose and that he was now terrified of the consequences.

A spokesman at the Pentagon's Defense Communications Agency, which has set up an emergency center to deal with the problem, said the caller's story was a ``plausible explanation of the events.''

As the virus spread Wednesday night, computer experts began a huge struggle to eradicate the invader.

A spokesman for the Defense Communications Agency in Washington acknowledged the attack, saying, ``A virus has been identified in several host computers attached to the Arpanet and the unclassified portion of the defense data network known as the Milnet.''

He said that corrections to the security flaws exploited by the virus are now being developed.

The Arpanet data communications network was established in 1969 and is designed to permit computer researchers to share electronic messages, programs and data such as project information, budget projections and research results.

In 1983 the network was split and the second network, called Milnet, was reserved for higher-security military communications. But Milnet is thought not to handle the most classified military information, including data related to the control of nuclear weapons.

The Arpanet and Milnet networks are connected to hundreds of civilian networks that link computers around the globe.

There were reports of the virus at hundreds of locations on both

coasts, including, on the East Coast, computers at the Massachusetts Institute of Technology, Harvard University, the Naval Research Laboratory in Maryland and the University of Maryland and, on the West Coast, NASA's Ames Research Center in Mountain View, Calif.; Lawrence Livermore Laboratories; Stanford University; SRI International in Menlo Park, Calif.; the University of California's Berkeley and San Diego campuses and the Naval Ocean Systems Command in San Diego.

A spokesman at the Naval Ocean Systems Command said that its computer systems had been attacked Wednesday evening and that the virus had disabled many of the systems by overloading them. He said that computer programs at the facility were still working on the problem more than 19 hours after the original incident.

The unidentified caller said the Arpanet virus was intended simply to ``live'' secretly in the Arpanet network by slowly copying itself from computer to computer. However, because the designer did not completely understand how the network worked, it quickly copied itself thousands of times from machine to machine.

Computer experts who disassembled the program said that it was written with remarkable skill and that it exploited three security flaws in the Arpanet network. [No. Actually UNIX] The virus' design included a program designed to steal passwords, then masquerade as a legitimate user to copy itself to a remote machine.

Computer security experts said that the episode illustrated the vulnerability of computer systems and that incidents like this could be expected to happen repeatedly if awareness about computer security risks was not heightened.

``This was an accident waiting to happen; we deserved it,'' said Geoffrey Goodfellow,''(*) president of Anterior Technology Inc. and an expert on computer communications.

``We needed something like this to bring us to our senses. We have not been paying much attention to protecting ourselves.''

Peter Neumann, a computer security expert at SRI International Inc. in Menlo Park International, said: ``Thus far the disasters we have known have been relatively minor. The potential for rather extraordinary destruction is rather substantial.

``In most of the cases we know of, the damage has been immediately evident. But if you contemplate the effects of hidden programs, you could have attacks going on and you might never know it.''

[* Following is Geoff's full quote ("exploitation"), which John only partially integrated with Geoff's earlier off-the-cuff comment ("accident"):

"This was an exploitation wanting to happen. We deserved it. We needed something like this to bring us to our senses. We have not been paying much attention to protecting ourselves. The blame does not rest on the R&D community as a whole. Look how many manufacturers [...] just took the original computer-science-department developed code willy-nilly, put their wrapper and corporate logo on it, and resold it to customers. That's the real travesty here, we build these systems, OK, that's great, but we rarely build them and then ask how they might be abused, broken, or circumvented" {and then try to break them}.]

"Annals of Democracy -- Counting Votes" in the New Yorker

Daniel B Dobkin <DAN%Irving@VX1.GBA.NYU.EDU>
Thu 3 Nov 88 11:18:09-EDT

The current (7 November 88) issue of The New Yorker contains an article by Ronnie Dugger on "Counting Votes" -- the spreading use of computerized vote tabulation in jurisdictions around the country. It confirms what we all know, or should know: the unprecedented potential for fraud, let alone the very real possibilities for "computer error", make this a giant step backwards for democracy and universal suffrage.

A number of the "experts" interviewed admitted that the potential for fraud -- or outright stealing the election -- exists, but brushed it off with a perfunctory, "I don't know of any cases yet where that has happened." To my mind, that is exactly the point: the fact that you don't know about it can just as easily be cited to indicate that it HAS happened; after all, you aren't SUPPOSED to know about it.

Other highlights of the article include interviews with Michael Shamos, formerly of UniLogic (now Scribe Systems); and Peter Neumann, of SRI International, the moderator of the RISKS digest.

Comments on the New Yorker article

Peter Neumann <neumann@kl.sri.com>
Thu, 3 Nov 1988 22:18:11 PDT

For the record, in Ronnie Dugger's interview with me, we discussed at length (1) the potential risks of using today's conventional computer system technology in elections, and (2) what one might do to try to develop a system that would avoid many of those risks -- although admittedly it could not be perfect. I presume that Howard Strauss (who is also quoted, and whose report "Ensuring the Integrity of Electronic Elections" with Jon Edwards outlines what they consider to be necessary procedural controls) also stressed his published recommendations. Apparently Dugger chose to emphasize the risks, and downplay discussion of constructive design techniques and operational procedures. He does note that New York City is currently engaged in the competitive procurement and development of a new system, but does not indicate that the specified requirements (e.g., complete enchipment, no software [and consequently no software modification], privacy, integrity, separation of duties, extensive redundancy and cross-checking, reproducibility of results, physical and electronic isolation, procedural controls, ...) are vastly more stringent that anything that exists today. So, perhaps the prospects for the future are substantially more optimistic than he has portrayed.

Incidentally, "A Special Report on Computing and Elections", 11 pp., a joint publication from ELECTION WATCH, a project of the Urban Policy Research Institute, and from the CPSR/Portland Computer Voting Project, Computer Professionals for Social Responsibility, is available from either CPSR, PO Box 717, Palo Alto CA 94301, 415-322-3778, or UPRI, 530 Paseo Miramar, Pacific

Palisades CA 90272, 213-459-4982. In addition, papers by Wilcox and Nilsson and by Strauss and Edwards are available for $5 (for both) from CPSR. The full report by Strauss and Edwards is available from Howard Strauss, 116 Prospect Ave., Princeton NJ 08544 for $8. Costs are for copying, handling, and postage only. [I have previously noted reports by Roy G. Saltman and by Lance J. Hoffman in RISKS-7.52.]

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 71

Sunday 6 November 1988

Contents

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

Send us your Arpanet Virus War Stories

Cliff Stoll <cliff@Csa4.LBL.Gov>
Sun, 6 Nov 88 04:29:26 PST

COLLECTING ARPANET VIRUS WAR STORIES

I'm collecting information about the Nov 3 Arpanet virus, trying to determine:

> How many sites were infected
> How many were not
> How quickly it spread

SO: If you were infected, please send me a note describing your experiences.
Please include:

> Where are you? What type of computers?
> What times were stamped on the /usr/tmp/x files?
> Which of your computers were infected? All of them?

Please send your anecdotes & stories, such as:

> What time did you discover it?
> What tipped you off?
> How did you and your colleagues respond?
> What would you differently?
> Did you call anyone? Or did anyone call you?
> Where would you turn for information next time?
> When did you finally eradicate it?
> Any weird wrinkles or strange effects?

I'm interested in hearing from you even if you were not infected!

Please pass this message on to others:
I would rather have multiple responses from a site than none.

Thank you very much for your time & trouble.
In return, I'll mail summaries to everyone that contributes.
If you want this, please include your address.

Thank you very much for your time & troubles!

Cliff Stoll Harvard/Smithsonian Center for Astrophysics
617/495-7147 60 Garden Street, Cambridge, MA 02138
Cliff@cfa200.harvard.edu (or on bitnet, Cliff@lbl) [Nov 5, '88]

[Cliff is presumably referring to the relevant UNIX systems only. I doubt he is interested in responses saying that your TOPS-20 or your PRIME or whatever was not hit, since the worm/virus was specific to certain DEC and Sun versions. (Thanks to Cliff for offering this service, although it further distracts him from his attempted pursuits of astronomy.) PGN]

Suspect in Virus Case

Brian M. Clapper <clapper@NADC.ARPA>
Sun, 6 Nov 88 14:55:20 EST

Reprinted (without permission) from the Philadelphia Inquirer, Sunday, November 6, 1988:

(From Inquirer Wire Services)
ITHACA, N.Y. - A Cornell University graduate student whose father is a top government computer-security expert is suspected of creating the "virus" that slowed thousands of computers nationwide, school officials said yesterday.

The Ivy League university announced that it was investigating the computer files of 23-year-old Robert T. Morris, Jr., as experts across the nation

assessed the unauthorized program that was injected Wednesday into a military and university system, closing it for 24 hours. The virus slowed an estimated 6,000 computers by replicating itself and taking up memory space, but it is not believed to have destroyed any data.

M. Stuart Lynn, Cornell vice president for information technologies, said yesterday that Morris' files appeared to contain passwords giving him un-authorized access to computers at Cornell and Stanford Universities.

"We also have discovered that Morris' account contains a list of passwords substantially similar to those found in the virus," he said at a news conference.

Although Morris "had passwords he certainly was not entitled to," Lynn stressed, "we cannot conclude from the existence of those files that he was responsible."

FBI spokesman Lane Betts said the agency was investigating whether any federal laws were violated.

Morris, a first-year student in a doctoral computer-science program, has a reputation as an expert computer hacker and is skilled enough to have written the rogue program, Cornell instructor Dexter Kozen said.

[... omitted details concerning Morris' unavailability for comment ...]

Reached at his home yesterday in Arnold, Md., Robert T. Morris, Sr., chief scientist at the National Computer Security Center in Bethesda, Md., would not say where his son was or comment on the case.

The elder Morris has written widely on the security of the Unix operating system, the target of the virus program. He is widely known for writing a program to decipher passwords, which give users access to computers.

[The remainder of the article basically restates information which has already been reported.]

Internet Virus

"Mark W. Eichin" <eichin@ATHENA.MIT.EDU>
Fri, 4 Nov 88 21:52:58 EST

A team at MIT and a team at UCB worked Thursday evening through until Friday morning both examining the Virus in isolation and reverse engineering to create C code that could produce the binary output we had in hand.

MIT had a Press Conference at 12Noon Friday, 4 November; about 20 minutes earlier, we had determined that with the modules we had received from Berkeley and the work we had done at MIT we indeed had a complete knowledge of the inner workings of the Virus, permitting us to declare that there was no code in the virus designed to harm files.

The Berkeley group was lead by Keith Bostic (I don't have details on his group); the MIT group was a collection of programmers from various organizations including Project Athena, LCS, SIPB, and Telecom. Stan Zanarotti and I led a group of around 6 in the reverse engineering effort, while others worked on using Netwatch on an isolated testbed machine.

The Virus uses three possible paths to transmit itself from one machine to another:

1) finger (via a bug in /etc/fingerd which turned out to be difficult for the Virus to exploit)

2) sendmail (via the `debug' command, which should be turned off in a production server, but apparently was turned on by default in the binary BSD distribution)

3) password guessing and shell/rexec/rsh/telnet logins.

Whichever method used, it attempted to run a /bin/sh on the remote machine, and then feed it a set of commands which caused it to build a new program and suck over an unlinked VAX or Sun image. It then linked this with the system's local libraries, and executed it.

Once the virus was running on the new site, it chose a variety of paths to find new hosts to propogate to:

1) routing tables
2) interface tables
3) user .forward files
4) user .rhosts files
5) /etc/hosts.equi

Note that it did *not* make any use of the inherent security problems commonly involved with .rhosts files, it merely used them as a source of hostnames.

[I'll cut this short now, I need the sleep...]

Project Athena was not vulnerable to the finger attack at all; one or two private machines were vulnerable to the `debug' attack, but at least one was an IBM RT/PC (which the Virus could `live' on.) What did hit several Athena machines was the use of password guessing; this is really more of a Human Security problem than a Computer Security problem. Other MIT machines were hit by various combinations of the several attacks.

There were several bugs in the Virus itself, which Keith Bostic suggested posting patches for. It also seems clear that the original design did not intend for it to hog resources as it did, but merely to propagate quietly, which would have certainly been interesting.

Very little effort was made to actually hide the behavior of the code (it even had a reasonably large symbol table, making it easier to identify subroutines.) It *did* attempt to hide at a higher level, for example by calling itself "sh" and destroying its argument list (to make it appear in the process table as ``some random shell script'').

I will try and post more details as I have time to write them up.

Mark Eichin
<eichin@athena.mit.edu>
SIPB Member & Project Athena ``Watchmaker''

RISKS of getting opinions from semi-biased sources

Brad Templeton <brad%looking.uucp@RELAY.CS.NET>
Sun Nov 6 15:50:07 1988

It's rare for the net to make the evening news, but I'm noting some interesting things.

Most of the media are jumping to "computer security experts" for comment on the matter. No offense, folks, but people who make their living from consulting on computer security are bound to perceive (and expound on) this as worse than it actually is. People are talking as though there's some surprising end-of-the-world potential in this event, when it really comes as no surprise to any RISKS reader, Internet or UNIX user.

University systems are designed, and should be designed as low-caution, high convenience systems. Such flaws *will* exist, and events like this only make us wiser. Remember the original unix documentation which detailed "how to bring UNIX to a halt if you're joe user" on page 1? Funny, but it never happens.

["What, Never?" "No, Never."
"What, Never?" "Hardly ever."
(Thanks to W.S.Gilbert) PGN]

The press will want sensationalistic answers, but if you're talking to them, try to steer them away from all the comments about "War Games." And clear up the use of the word "hacker" now that things are in the public eye!

Brad Templeton, Looking Glass Software Ltd. -- Waterloo, Ontario 519/884-7473

Semi-biased sources

Peter G. Neumann <Neumann@KL.SRI.COM>
Sun, 6 Nov 88 22:01:17 PST

This episode has given system administrators and users the opportunity to recall that there are many lurking vulnerabilities. But to assume that university computing should be relatively wide open would be a serious mistake. Unethical and other abuses are not uncommon. There is plenty of proprietary research, and there are serious integrity problems. NASA contemplates permitting a professor sitting at his workstation to up-link via network to the space station and control his experiments in real-time. So can anyone else who happens to subvert the local system or its communications. Intruders might even be able to bring down the space station itself by penetration techniques. Also, students writing theses would not like to see their files deleted and their backups made unretrievable by premeditated contamination resulting from a long-standing but not yet detected Trojan horse. Note that many problems could arise accidentally rather than maliciously. In some cases accidental damage can be just as severe as intentional damage. (See my comments on the 1980 ARPANET fiasco, below.) It seems that the valuable lessons that should be derived from the worm/virus would be totally lost if we continue with business as usual (although presumably at least the flaws already exposed will have been

patched, now that they are suddenly more widely known). Furthermore, significant improvements in security are in the offing -- including various considerably more secure versions of UNIX. (And amazingly, performance and ease of use need not be seriously compromised!) I think that a university computing administrator would be strung up after an installation known *a priori* to be badly flawed was attacked, especially if much better systems or better operational procedures had been available and commonly used elsewhere. Perhaps I am flogging a straw herring in mid-stream, but in the light of what is known about the ubiquity of security vulnerabilities, it seems vastly too dangerous for university folks to run with their heads in the sand. [It is not ostrich of the imagination to contemplate future attacks that are really malicious. And yes, they do happen and have happened.] So, despite the the worm/virus having caused considerable pain, it does have the potential for having been a useful exercise -- if anyone is listening and thinking.

Worm/virus mutations

"David A. Honig" <honig@BONNIE.ICS.UCI.EDU>
Sun, 06 Nov 88 14:24:09 -0800

The resource-hungry arpanet worm was supposedly a mistake: it was not supposed to use resources as fast as it did. This was a design (programmer's) error, I think.

I'm interested in how difficult it would have been for the intended mild worm to "mutate" into the system-stopping one. In particular, what would a mild version look like, and what kind of error in reproduction would transform from the hungry worm into the milder one?

Would simply removing a line of text from one of the scripts have worked? Would a single undetected bit error in one character have made a difference? (What if that error commented-out an entire line of a file?) I expect most mutations would be fatal or sterilizing at least, but if a net-infection were to persist uncured for a while, it is possible (and as time progresses, probable) that mutated strains would occur, and some fraction of these would be nastier than their ancestors.

Re: Worm/virus mutations

Peter G. Neumann <Neumann@KL.SRI.COM>
Sun, 6 Nov 88 21:27:39 PST

In general, the difference between killer and benign could be one bit. The ARPANET crash of 27 Oct 1980 resulted from bits accidentally being dropped in the time stamp of one status word. The resulting multiplicity of three versions (two corrupted) of the same status word (with different time stamps) broke the garbage collection algorithm, and degraded the ARPANET to ZERO. (See ACM SIGSOFT Software Engineering Notes Jan 1981 for discussion of the data retrovirus.)

The UNIX worm/virus would have been relatively harmless (and much less

detectable) had its creator not attemped to make it survivable even after detection and removal. The choice of a parameter invoking a one-in-ten reinfection was what made it degrade each attacked system.

Worm sending messages to ernie.berkeley.edu?

Jacob Gore <gore@eecs.nwu.edu>
Sun, 6 Nov 88 16:36:52 CST

From The New York Times (National), Sunday, Nov. 6:

> Mr. Morris learned of his replication error through a monitoring mechnanism [sic] he had built into his program. Each second each virus broadcast its location to a computer named Ernie at the University of California at Berkeley, said a computer researcher who has analyzed the virus.

Is this true? If so, what account were the logs sent to?

Jacob Gore Gore@EECS.NWU.Edu
Northwestern Univ., EECS Dept. {oddjob,gargoyle,att}!nucsrl!gore

---

Re: "UNIX" Worm/virus (RISKS DIGEST 7.70)

Peter da Silva <peter@sugar.uu.net>
5 Nov 88 19:31:58 CST (Sat)

> decwrl!ucbvax!KL.SRI.COM!RISKS

I realise that for most of the people in the Internet UNIX == 4.2, but people should be more careful of referring to bugs in the UNIX operating system. While there may be bugs in any operating system, this virus didn't exploit any UNIX bugs.

First, the actual bug is implicit in a mailer program, sendmail. This isn't "The UNIX operating system", and it's not even found on most systems.

Secondly, the other "bugs" are security holes deliberately left open to make network operations more convenient when dealing with other trusted machines. Again, this isn't a bug in UNIX.

Finally, a channel like this can't be used to infect non-BSD systems without the debug version of sendmail, unless individual users choose to set up "shell deamons" to watch their mailboxes. This falls under case 2 above.

Referring to this is a UNIX virus is going to give naive users the idea that UNIX is particularly susceptible to penetration over a network. Our management has expressed concern, for example, that our own Usenet feed could be used to infect us.

Yes, it could... given a sufficiently subtle trojan horse hidden in, say, a comp.sources distribution. But that's not a *UNIX* or *Network* problem...

we're more susceptible to people bringing in diskettes.

The last thing we need now is the UNIX equivalent of the "Audi sudden acceleration" panic.

Peter da Silva `-_-' peter@sugar.uu.net

Comments on vote counting

<wcs@alice.att.com>
Sat, 5 Nov 88 23:24:33 EST

Several people have commented on the risks of computerized vote tabulation, but there's another RISK here - inaccurate and fraudulent reporting.

The National Election Service, which is the joint election reporting group funded 20% each by CBS, NBC, ABC, AP, and UPI, has announced that they will not report any third-party results for the presidential elections this year. Ron Paul, the Libertarian Party candidate, asked how they would report a 45%-45%-10% vote (if he gets 10% of the vote in Alaska, an LP stronghold) - they replied "We'll call that 50-50".

This sort of thing has a major effect on voters' perceptions of the elections - if they never hear about alternatives to the status-quo parties, they're unlikely to vote for them in the future. This could get especially interesting if Lenora Fulani's New Alliance Party succeeds in their lawsuit to keep the Democratic and Republican parties off the Indiana ballot (where they filed late) - they may get all the electoral votes unless there is substantial write-in voting.

Bill Stewart, att!ho95c!wcs, AT&T Bell Labs Holmdel NJ 1-201-949-0705
and/or
Shelley Rosenbaum, att!ho95c!slr, 1-201-949-3615 ho95c.att.com

Re: A320 update

<attcan!utzoo!henry@uunet.UU.NET>
Sun, 6 Nov 88 02:08:09 EST

>Henry Spencer's recent article on the A320's first six months in
>service states that the fly-by-wire system has "behaved perfectly."
>It should be noted, however, that the article he was referring
>to clearly pointed out that there were failures of the primary
>flight guidance computer, which were rectified by backup systems.

Hardware failures, dealt with by backup systems, happen even in non-computerized aircraft. With substantial frequency, in fact. This did not seem worth mentioning. As nearly as I can tell from that article, and the later ones, there have been no major *software* problems in the flight-control software... which is what everyone was worried about. Hardware failures are to be expected.

>I find Ziegler's rationale for the failures of the A320 somewhat
>disturbing. With only a handful of airplanes in service, for any
>significant percentage of in-flight or on-ground failures to occur,
>and then say it should be compared to the massive fleets of existing
>aircraft, is to obfuscate the issue.

How so? Note that he is citing *percentages of flights* delayed, not absolute counts; fleet size is irrelevant except insofar as statistics over a small fleet are less precise than over a large fleet. His comments about media attention are more dubious in this regard, since occasional failures in a small fleet are indeed more significant than the same failures-per-day rate would be in a large fleet, but even there I think he's got a point: if ten 747s fail per day, nobody cares, but if an A320 fails once every two weeks, it's a scandal.

>His confidence in the A320's backup electrical systems is also rather
>odd, considering the airplane's susceptibility to transient controls,
>and his company's failure to provide even a mediocre cabin lighting
>control system.

Notice that the transient problems are (as far as I've heard) all in non-critical support systems, and the cabin-lighting-control problem is with a subcontractor, presumably not the same people who did the main electrical system. Agreed that Airbus is responsible in the end, but the implication that these problems spill over into more critical systems seems unjustified.

Henry Spencer at U of Toronto Zoology uunet!attcan!utzoo!henry

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 72

Tuesday 8 November 1988

Contents

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

The Worm/Virus -- and an Unlearned Lesson

Peter G. Neumann <Neumann@KL.SRI.COM>
Tue, 8 Nov 88 14:03:20 PST

There have been OVER 50 MESSAGES to RISKS since last evening, and over a hundred backlogged since Friday. Bear with me. I'll get to them. I am only human, although I try to be that as well as I can. Things have been fairly hectic here.

Not surprisingly, most of the pending messages deal with the RTM worm/virus discussion, which continues with healthy discussion on propriety, morality, ethics, prosecution, judgement, compensation, penance, etc. The messages are

vastly too repetitive to include fully, and range wildly all over the map -- from "string him up" to "let's learn the lessons he has offered for us." The discussion is indeed very worthwhile, but needs significant editing to make it palatable to our usually discriminating audience. Thus, I thought it might be nice to have an issue on other subjects while I am trying to get the worm material together. Here is a potpourri of backlog.

By the way, something approaching a hundred copies of RISKS-7.69 -- which have been queued since Friday -- are still waiting on my system for the recipient systems to accept delivery. (RISKS-7.70 and 71 also.) I assume many sites are STILL off the (ARPA|MIL) net. Worse yet, we had need today to poke at a UNIX system that claims to be up on the ARPANET but was rejecting mail. SMTP showed the system working. But, guess what? The DEBUG option still works fine on that system! I wonder how many other system administrators have still not learned anything yet.

Airline Reservation System Vulnerabilities

Rodney Hoffman <Hoffman.es@Xerox.COM>
4 Nov 88 12:33:11 PST (Friday)

Today's "Wall Street Journal" carries a story about American Airlines suing a Tulsa, OK woman and her father who have credit for more than 50 million miles in American's frequent flier program. The airline alleges that they and unknown co-conspirators stole the mileage by breaking into American's computer reservations system. They have also been indicted by a federal grand jury for wire fraud in the alleged scheme.

The woman is an independent employee of a travel agency. She is accused of shifting miles from actual travelers who were not part of American Airlines frequent flier program into fake frequent flier accounts, then redeeming for tickets and selling those.

But the story concludes with some more general worries:

> The allegations raise some troubling questions about access to airline computer systems. Such systems contain a wealth of information not only about frequent-flier trips, but also about the confidential travel plans of hundreds of companies. And yet any employee at any travel agency can normally log into the agency's system and see any trips the agency has booked.
>
> "It's just too easy to get into these systems," says John Caldwell, a travel attorney in Washington, D.C. "I think this is going to become an increasingly sensitive issue."

Computers in the oldest profession

Dave Horsfall <dave@stcns3.stc.oz.au>
Wed, 2 Nov 88 13:14:59 est

From the "Backbytes" page in Computing Australia, 31st Oct 88:

``Where the Gigabyte meets garter belt

As computer and related industry manufacturers scout for new niche markets, they could do worse than consider the world's oldest profession. In recent months, US cops have busted several large prostitution rings -- all heavily dependent on microcomputer support. The databases held such priceless information as clients' names and addresses, billing methods, preferred frolics and the names of who did what best. And to whom.

How the new technocrats had missed the lucrative sales possibilities to this service industry is hard to fathom, as one recently raided establishment of easy virtue was in San Jose, in the heart of California's Silicon Valley. In its computer's ledger were the names of more than 50,000 customers. Obviously, a considerable horizontal market worth the attention of a lateral-thinking, but discreet, sales go-getter.''

Auto Privacy

DAVE ROBINSON DTN:830-6498 REO2-G/C2 <robinson%osi.DEC@decwrl.dec.com>
Fri, 4 Nov 88 01:43:49 PST

In recent issues of RISKS there has been concern voiced over the ability to trace the location of a car from its car phone. Last night, no BBC's TOP GEAR programme, a device deliberately designed to locate cars was described. Essentially, it is a navigational aid designed to take into account traffic congestion.

You tell the device your intended destination and it determines the best route. On the way, it tells you when the turn right or left both on a dashboard indicator and a synthesised voice. So far, nothing particularly revolutionary.

The route selected takes into account the traffic congestion on various roads. To determine this, there are many sensors across a town. When you pass one of these sensors, the device in your car sends a message to it. Each sensor is connected to a central computer. This records the time taken to travel from one sensor to another to judge the current congestion alone the route. However, the side effect is that the central computer knows our location and route through a city. This loss of privacy would be even greater should the scheme be extended to cover not only the individual cities but also the interconnecting motorways and side roads.

At present, the scheme is only in prototype. It is being developed at the Goverment's Road Research Laboratories. However, it does indicate the sort of devices we may be getting in the future.

To the best of my knowledge, Digital Equipment Co. has no involvement in the project. Hence the usual disclaimers apply.

Dave Robinson

computer science unencumbered by fears about cutting safety margins

Jeffrey Mogul <mogul@decwrl.dec.com>
2 Nov 1988 1742-PST (Wednesday)

I had to spend a few hours at the British Airways terminal at Heathrow last week, and to help kill time I picked up a copy of the October 1988 issue of a free magazine called "Airport". The cover story is "Fighting for the Freedom of the Skies: In Europe ...", and covers the European experiences with their version of airline deregulation. Apparently, the fragmented and uncoordinated nature of European Air Traffic Control is causing chaos (my own flight was delayed by ATC for 45 minutes, and our pilot told us as we left that flights requesting clearance at that time were being told to wait for 90 minutes).

The final two paragraphs of the article made me chuckle (nervously):

> Aviation Scientists in Britain, the US, France and West Germany are now working on a data-exchange system which would reduce or even eliminate the human element in air traffic control and in airport approach, landing and take-off-slot technique.

[so far, so good]

> Machine-talking-to-machine would enable the system to improve perhaps five-fold, because the precise nature of computer science is unencumbered by fears about cutting safety margins too finely. A cold dish of comfort, perhaps; one which will not be available until well after 2005. And anyway, nobody knows yet how much such a system will cost. But we all know who's going to pay for it, don't we?

The syntax of the first sentence is a little confusing, but I think the author believes that once things are computerized there will be no need for safety margins. Computerization might well reduce the need for safety margins, but this has little to do with how precise computer science is (or is alleged to be).

Re: Risks in Answering Machines (revisited) (RISKS DIGEST 7.68)

Amos Shapir <amos@taux02.UUCP>
2 Nov 88 13:16:44 GMT

Andy-Krazy-Glew writes:
> (3) Have there been any incidents of remote sabotage of answering machines,
> or, worse, criminal interception of messages, or bugging, as I describe
> above?

During the latest election campaign here, one of the major parties set up several answering machines for political messages, e.g. "if you want to know why you should vote for us, dial 555-1234". They were very surprised when they found out that the messages have been changed, (not in their favor of course).

The machines were rented from a company that lets users have only a phone number to call to, and an access code; so the only way such messages may have been altered is by remote control.

Amos Shapir, National Semiconductor (Israel) P.O.B. 3007, Herzlia 46104, Israel

---

re: risks in answering machines (revisted)

Gordon Meyer <TK0GRM1@NIU.BITNET>
Wed, 02 Nov 88 12:38 CST

Andy Glew expresses some concerns about the security of telephone answering machines. I too have these concerns, and have had some problems along these lines with my answering machine at home. It is an older Cobra model. Manufactured in about 1982 it offers remote message retrieval with the use of a tone generating device. The remote control device is a pain to use...you have to carry it around with you, and past experiments have shown that tone units from other machines will work just as well as the one the company provides! A friend of mine had a similar machine, of another brand, and our remote controls worked interchangably. Also, I did a little experimenting and found that I could activate both our machines by using a sweeping tone generated by my home computer.

About six months ago I had a problem with an unknown person calling my machine and listening to my messages. There was no way I could disable this option, but there is a switch that prevents outside callers from erasing the messages after listening to them. There is no option to change outgoing messages and the like so that is not a concern with this machine. Luckily I have since moved and the new phone number has stopped these outside invasions of my privacy.

A back issue of 2600 Magazine had a short editorial on this subject. Their response to the uncaring attitude of the manufacturer was to call the company at night, (the company was using their own machines to man the phones at night) and change the outgoing message to one warning others about the lack of security on the product.

Gordon R. Meyer, Dept of Sociology, Northern Illinois University.

Re: RISKS DIGEST 7.68 (Answering machines)

Bob Felderman <feldy@ats.ucla.edu>
Mon, 31 Oct 88 18:38:24 PST

The cobra AN-8500 allows ONLY remote listening to messages and has a switch on the machine which determines whether msgs will be erased after being heard remotely. Unfortunately, the code for remote listening is one (1) factory preset digit.

Bob Felderman feldy@cs.ucla.edu
UCLA Computer Science ...!{rutgers,ucbvax}!cs.ucla.edu!feldy

re: Risks in Answering Machines (revisited)

GREENY <MISS026@ECNCDC.BITNET>
Mon 07 Nov 1988 00:56 CDT

> Are there any machines on the market.....

Well, the one that I have (mainly for cost reasons, since I'm just an undergrad) is a Phonemate. Basically, it answers the phone, plays my digitally recorded message, and takes the message.....then when I come home I can listen to them.

About the only thing that it does remotely is answer the phone, and get my messages. Although it does allow one to turn it on (if its accidently let off) from a remote location by letting the phone ring 15 times or more (it will pick up and play the message to let you know that it is on.....).

After being on RISKS for a few years, I have realized that the convience realized by a completely remote machine is not worth the risks. I suppose I could always go to voice mail, or hire a secretary if I needed one....

> Is there any machines out there w/o the remote erase....

What's the big deal? The machine *usually* has a cassette, in it, and assuming that it wont do a remote rewind of the cassette after playback, all one would have to do to disable the erase circuit would be to install a small switch in series with the erase head....when you go out, flip it off when you come back in and want to erase -- flip it on. GEtting a copy of the schematics would be helpful if possible so that you could disable the entire circuit thereby preventing the thing from rewinding w/o erasing and then taping over the messages....perhaps a circuit that would prevent erasure during rewind (the way they usually work) so that you could play them back but not erase em (i.e. it wouldnt rewind or erase if you selected erase with the "switch" off....

Shouldn't be too much of a hassle if you are somewhat knowledgeable in electronics.....or if you arent -- try to find a hungry student in electronics and offer PIZZA! :->

Greeny

Bitnet: miss026@ecncdc
Internet:miss026%ecncdc.bitnet@cunyvm.cuny.edu
Disclaimer: I ain't responsible for nothing you or anyone else does...so don't blame me....

Re: Risks in Answering Machines

<Curtiss@DOCKMASTER.ARPA>
Wed, 2 Nov 88 14:03 EST

In RISKS 7.68, Andy "Krazy" Glew asks if there are any answering machines with redefinable passwords that are long enough for an acceptable level of security and if any have only non-destructive remote commands. One possible solution is an "answering machine card" for a PC. Essentially, it is a complete telephone interface, capable of recognizing touch tones, recording and playing digitized speech (stored on a hard disk or floppy) and acting as a modem. A program is usually included with the board that makes it function as an answering machine. Since the full power of a complete computer is available, the user can create any kind of password scheme they desire, including multi-level menus for leaving messages for specific people. Also, the program can be modified to eliminate destructive remote commands and new functions can be added. They can even be set up to call people, delivering a pre-recorded message (ala, computer cold calling).

There are two such boards available, that I know of. Either can be had for about $250, not much more than a full featured, top-of-the-line dedicated machine.

I'm not quite sure that this is a good solution to the problem, though. Now we have a potentially expensive machine attached to the phone line. If you're worried about losses to messages on a dedicated tape, just think about the PC with one of these cards.

William Curtiss

<cmcl2!cucard!dasys1!eravin@harvard>
Thu, 3 Nov 88 15:42:07 EST

> That noise is *very* nasty; there really ought to be emissions standards.
> Every low-cost computer I've ever worked with has been horribly annoying.
> IBM PC's with CGA cards (or EGA cards in CGA mode) were terrible offenders;
> even my Mac is fairly offensive.

I used to shudder when I heard an IBMPC go into EGA graphics mode. On my current job that happens ten or twenty times a day, I still don't like it but I'm used to it. I love using the Mac but do notice the noise: sometimes it helps on a lot of these monitors to hang a cloth or drape something soft behind the machine. When the monitor is backed against a solid wall the problem is usually worse. I also have noticed noise coming out of a couple of IBM AT clone's power supplies, though not at irritating frequencies.

> (High-resolution screens (noninterlaced, 640x480 and up) don't seem to
> have the problem, but they won't become common in cost-sensitive
> applications for quite a while.)

I don't agree with this. I think you just can't hear them anymore because they're using higher scan rates. My usually reliable intuition has steered me away from a Sun workstation with a 19" color screen. However, working with Unix PC's has really sensitized me to this stuff: when I was last abroad I had trouble being in the same room as a European TV set (625 scan lines), especially 25" models.

> How can we drum up some pressure to get OSHA to look into this?

Good question. I've never thought about it, but I sure would like to try. I suspect letters and phone calls to one's favorite senator or representative would be a start. Might even be worth trying...

-- Ed Ravin

Reader bears responsibility for all opinions expressed in this article.

Ultrasonic emissions a real problem

Geoffrey Welsh <izot@f171.n221.z1.fidonet.org>
Mon, 07 Nov 88 18:13:29 EST

In RISKS-7-68 eravin@dasys1.UUCP (Ed Ravin) writes:

>I've got my own story to tell about high frequency noises crawling out of
>computer related devices, and since I'm new to RISKS, my apologies if any
>or all of this has been discussed before.

I, too, am new to RISKS (drawn here by news of the ARPAnet worm), and I, too, share your earitability. (sorry!)

When I was much younger, I used to hear whistle sounds and I'd ask my parents what they were. They immediately took me to the doctor, who told them that I did *not* have an ear infection. They stopped only short of taking me to a neurologist to find out if something upstairs was shorting out.

>After that I began noticing the sounds made by all the other CRT's in my
>life. They were high pitched and slightly irritating, but not painful. I had
>always, even before meeting computers, noticed the 15khz whine from a TV set,
>but it had never bothered me.

It didn't take me long to figure out that this was among the causes of the noise I was hearing. I have also heard sounds which are distinctly higher in pitch than a standard NTSC CRT (i.e. higher frequency than a 15,750 Hz flyback transformer). I am puzzled as to exactly what these are as the only things I know of that operate around 16 KHz RF are LORAN-type devices and, to the best of my knowledge, I am near no such installations (e.g. the nearest sizable body of water is a long drive from here).

>Maybe my problem is that I never listened to loud rock music and my hearing
>above 15khz is mostly intact.

Here's the kicker: I HAVE listened to loud rock music. I have worked in factories where a wide spectrum of loud noises assaults me for eight or twelve hours at a time (with occasional breaks), but my inability to hear these high frequencies clearly fades within an hour or so after I leave, leading me to believe that that my decreased hearing sensitivity is more a muscle reaction in my ear rather than damage cause by the volume.

What, then, leads some of us to be sensitive to these frequencies to a fault and others to be completely unaware of them? Worse, how can we determine what levels are acceptable, given that some people are simply more sensitive than others?

If indeed ultrasonic emissions are a cause of illness or other unacceptable consequences, it is vital that a study into the area be launched. Who knows; in a few years we may find our present CRTs replaced with ones that have a horizontal scan rate above 30 KHz to avoid this problem.

Geoffrey Welsh, 66 Mooregate Crescent, Suite 602, Kitchener, Ontario N2M 5E6 - CANADA

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 73

Wednesday 9 November 1988

Contents

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

NYT/Markoff: The Computer Jam -- How it came about

the tty of Geoff Goodfellow <geoff@fernwood.mpk.ca.us>
Tue, 8 Nov 88 21:40:00 PST

THE COMPUTER JAM: HOW IT CAME ABOUT
By JOHN MARKOFF
c.1988 N.Y. Times News Service, 8-Nov-88

Computer scientists who have studied the rogue program that crashed through many of the nation's computer networks last week say the invader actually represents a new type of helpful software designed for computer networks.

The same class of software could be used to harness computers spread aroun the world and put them to work simultaneously.

It could also diagnose malfunctions in a network, execute large computations

on many machines at once and act as a speedy messenger.

But it is this same capability that caused thousands of computers in universities, military installations and corporate research centers to stall and shut down the Defense Department's Arpanet system when an illicit version of the program began interacting in an unexpected way.

``It is a very powerful tool for solving problems,'' said John F. Shoch, a computer expert who has studied the programs. ``Like most tools it can be misued, and I think we have an example here of someone who misused and abused the tool.''

The program, written as a ``clever hack'' by Robert Tappan Morris, a 23-year-old Cornell University computer science graduate student, was originally meant to be harmless. It was supposed to copy itself from computer to computer via Arpanet and merely hide itself in the computers. The purpose? Simply to prove that it could be done.

But by a quirk, the program instead reproduced itself so frequently that the computers on the network quickly became jammed.

Interviews with computer scientists who studied the network shutdown and with friends of Morris have disclosed the manner in which the events unfolded.

The program was introduced last Wednesday evening at a computer in the artificial intelligence laboratory at the Massachusetts Institute of Technology. Morris was seated at his terminal at Cornell in Ithaca, N.Y., but he signed onto the machine at MIT. Both his terminal and the MIT machine were attached to Arpanet, a computer network that connects research centers, universities and military bases.

Using a feature of Arpanet, called Sendmail, to exchange messages among computer users, he inserted his rogue program. It immediately exploited a loophole in Sendmail at several computers on Arpanet.

Typically, Sendmail is used to transfer electronic messages from machine to machine throughout the network, placing the messages in personal files.

However, the programmer who originally wrote Sendmail three years ago had left a secret ``backdoor'' in the program to make it easier for his work. It permitted any program written in the computer language known as C to be mailed like any other message.

So instead of a program being sent only to someone's personal files, it could also be sent to a computer's internal control programs, which would start the new program. Only a small group of computer experts _ among them Morris _ knew of the backdoor.

As they dissected Morris's program later, computer experts found that it elegantly exploited the Sendmail backdoor in several ways, copying itself from computer to computer and tapping two additional security provisions to enter new computers.

The invader first began its journey as a program written in the C language. But it also included two ``object'' or ``binary'' files -- programs that could be run directly on Sun Microsystems machines or Digital Equipment VAX computers without any additional translation, making it even easier to infect a computer.

One of these binary files had the capability of guessing the passwords of users on the newly infected computer. This permits wider dispersion of the rogue program.

To guess the password, the program first read the list of users on the target computer and then systematically tried using their names, permutations of their names or a list of commonly used passwords. When successful in guessing one, the program then signed on to the computer and used the privileges involved to gain access to additonal computers in the Arpanet system.

Morris's program was also written to exploit another loophole. A program on Arpanet called Finger lets users on a remote computer know the last time that a user on another network machine had signed on. Because of a bug, or error, in Finger, Morris was able to use the program as a crowbar to further pry his way through computer security.

The defect in Finger, which was widely known, gives a user access to a computer's central control programs if an excessively long message is sent to Finger. So by sending such a message, Morris's program gained access to these control programs, thus allowing the further spread of the rogue.

The rogue program did other things as well. For example, each copy frequently signaled its location back through the network to a computer at the University of California at Berkeley. A friend of Morris said that this was intended to fool computer researchers into thinking that the rogue had originated at Berkeley.

The program contained another signaling mechanism that became its Achilles' heel and led to its discovery. It would signal a new computer to learn whether it had been invaded. If not, the program would copy itself into that computer.

But Morris reasoned that another expert could defeat his program by sending the correct answering signal back to the rogue. To parry this, Morris programmed his invader so that once every 10 times it sent the query signal it would copy itself into the new machine regardless of the answer.

The choice of 1 in 10 proved disastrous because it was far too frequent. It should have been one in 1,000 or even one in 10,000 for the invader to escape detection.

But because the speed of communications on Arpanet is so fast, Morris's illicit program echoed back and forth through the network in minutes, copying and recopying itself hundreds or thousands of times on each machine, eventually stalling the computers and then jamming the entire network.

After introducing his program Wednesday night, Morris left his terminal for an hour. When he returned, the nationwide jamming of Arpanet was well under way, and he could immediately see the chaos he had started. Within a few hours, it was clear to computer system managers that something was seriously wrong with Arpanet.

By Thursday morning, many knew what had happened, were busy ridding their systems of the invader and were warning colleagues to unhook from the network. They were also modifying Sendmail and making other changes to their internal software to thwart another invader.

The software invader did not threaten all computers in the network. It was aimed only at the Sun and Digital Equipment computers running a version of the Unix operating system written at the University of California at Berkeley. Other Arpanet computers using different operating systems escaped.

These rogue programs have in the past been referred to as worms or, when they are malicious, viruses. Computer science folklore has it that the first worms written were deployed on the Arpanet in the early 1970s.

Researchers tell of a worm called ``creeper,'' whose sole purpose was to copy itself from machine to machine, much the way Morris's program did last week. When it reached each new computer it would display the message: ``I'm the creeper. Catch me if you can!''

As legend has it, a second programmer wrote another worm program that was designed to crawl through the Arpanet, killing creepers.

Several years later, computer researchers at the Xerox Corp.'s Palo Alto Research Center developed more advanced worm programs. Shoch and Jon Hupp developed ``town crier'' worm programs that acted as messengers and

``diagnostic'' worms that patrolled the network looking for malfunctioning computers.

They even described a ``vampire'' worm program. It was designed to run very complex programs late at night while the computer's human users slept. When the humans returned in the morning, the vampire program would go to sleep, waiting to return to work the next evening.

[Please keep any responses short and to the point. PGN]

Single-bit error transmogrifications

Robert D. Houk <houk@sli>
Tue, 8 Nov 88 13:50:34 EST

[This started out with a question from Robert on mutations. My answer to him (not in RISKS) included this fragment:
In general, the difference between killer and benign could be one bit. The ARPANET crash of 27 Oct 1980 resulted from bits accidentally being dropped in the time stamp of one status word. ... PGN]

Another example of a one-bit error that escaped all error-detection to wreak havoc: A DQ-11 [am I dating myself?] would very occasionally (every month or so) drop a leading "0" bit at the begining of a message it was transmitting (this being a DDCMP protocol point-to-point network called "ANF-10" running under the TOPS-10 operating system). If this bit stream happened to also end in a "0" bit, the net effect was to "left-shift" the entire message by one bit. This not only slipped by the CRC checks, it resulted in a legally-formatted message as well! In particular, a random data message was transmogrified into a network protocol START message. The receiving node saw the START, and did the normal communications restart, including sending the START-ACK to the other side, which promptly went ??WHAT??, took its line down, and restarted communications with a real START message. The net effect (for this particular customer/network) was an out-of-the-blue transient network partitioning (they had no alternate routing paths, so all user connections were lost in the partitioning), with no errors detected or reported anywhere to account for it!

Now, while we were all pretty amused (yea, even amazed) at such arcana, I recall the customer being more of the opinion that it was a "killer" and not all that amusing. A new DQ-11 fixed the problem.

-RDH

New news from Hacker attack on Philips France, 1987

Klaus Brunnstein <brunnstein%rz.informatik.uni-hamburg.dbp.de@RELAY.CS.NET>
07 Nov 88 12:49 GMT+0100

A German TV magazine reported (last week) that the German hackers which attacked, in summer 1987, several computer systems and networks (including NASA, the SPANET, the CERN computers which are labeled `European hacker center', as well as computers of Philips France and Thompson-Brandt/France) had

transferred design and construction plans of the MegaBit chip having been developed in the Philips laboratories. The only information available is that detailed graphics are available to the reporters showing details of the MegaBit design.

Evidently it is very difficult to prosecute this data theft since German law does not apply to France based enterprises. Moreover, the German law may generally not be applicable since its prerequit may not be true that PHILIPS' computer system has `special protection mechanisms': evidently, the system was only be protected with UID and password, which may not be a sufficient protection (and was not).

Evidently, the attackers had much more knowledge as well as instruments (e.g. sophisticated graphic terminals and plotters, special software) than a `normal hacker' has. Speculations are that these hackers were spions rather than hackers of the CCC which was blamed for the attack. Moreover, leading members of CCC one of whom was arrested for the attack, evidently have not enough knowledge to work with such systems.

Klaus Brunnstein, Hamburg, FRG

Re: Telephone answering machines

<Curtiss@DOCKMASTER.ARPA>
Wed, 9 Nov 88 09:18 EST

In RISKS-7.69 Vince Manis states that his answering machine has an 8-bit octal security code for a search space of 256. He is not worried about someone breaking into his machine since "people aren't patient enough to call a number 256 times just to break in." Well, someone who is really determined would and with a computer and War Games dialer it even wouldn't be that terrible. However, even that is not necessary. Only TWO phone calls should be sufficient. Most answering machines do not care about wrong access codes or noise around a correct one -- they just ignore the extra digits. As long as the incoming stream contains the code somewhere you are given access. Since 256 in octal needs three digits, a carefully constructed string of 258 digits will contain every possible combination (for example, if the code is a triplet composed of just the numbers 1 and 2 then the string 1211122212 contains all eight triplets). Since the normal true-tone phone generates a pulse 70 milliseconds long with inter-digit spacing of the same (some phones continue generating the tone as long as the digit is held down, but these are near the minimum -- perhaps someone more knowledgeable in the matter can provide us with the guaranteed minimum) or 7.14 digits per second. So, I only need just over 36 seconds to try all codes. Since your machine might not be this patient, I could do it in two 18 second calls. Of course, I can't dial this fast, but my modem can.

William Curtiss

> [And there is a large literature on polynomially generated shift-register sequences that have the desired property. I would say that is a rather vulnerable design for use in sensitive applications, but perhaps adequate

if you have no secrets to hide and would not be concerned with maliciously deleted messages. Note that denials of service -- e.g., total saturation of our answering machine tape -- can be achieved without access to the security code. PGN]

Fly by Light

Martyn Thomas <mct@praxis.UUCP>
Mon, 7 Nov 88 13:02:42 BST

Flight International (November 5th 1988) reports the successful maiden flight on October 23rd of the Airship Industries Skyship 600-04 - which uses the world's first full-authority fly-by-light flight control system.

The fly-by-light system, developed by GEC Avionics, uses fibre-optics, which are highly resistant to electromagnetic interference and lightening strikes.

Martyn Thomas !uunet!mcvax!ukc!praxis!mct

---

decompiled viruses

Dave Pare <mr-frog@fxgrp.UUCP>
Fri, 4 Nov 88 17:22:33 PST

Last night a massive effort to decompile the "internet virus" was made by half a dozen people working at the CSRG in Berkeley. Most of the code is complete now, and most of the guesses that people have made were right on insofar as how it works, what it targets, and how it is distributed.

Precautions were taken by the author to clean up intermediate files, to use XOR functions on program strings, repeated forks, making many static procedures and using the linker to remove (presumably) suspicious-looking procedure names, naming the program "sh", etc, in order to better protect the program from detection and identification. This was definitely a deliberate action; quite a number of precautions were taken to hide the process.

The program was also fairly sophisticated in concept. It doesn't appear that the primary *motivation* of the author was the overloading of the target machine. There were several bugs encountered during decompilation, (most notably a "bzero(foo, sizeof(foo))", where foo is a struct) which may have accounted for the program's obnoxious and apparently unintentional behavior.

In my opinion, had the author tested this program more completely, it would have been quite a while longer before it was detected. While this incarnation of the program was a serious nuisance, a correctly-working version would have been far more insidious. It would have required a very curious system manager to notice an "innocuous" daemon listening to an unusual internet port number, or strange-looking messages in the sendmail syslog.

When someone who really knows how to code finally writes one of these things, we may never find out about it until weeks or months later. Although this program doesn't modify existing programs on affected systems, future ones might -- heck, they may have already done so.

Dave Pare

Worms/viruses/moles/etc. and the risk of nuclear war

"Clifford Johnson" <GA.CJJ@Forsythe.Stanford.EDU>
Mon, 7 Nov 88 18:44:33 PST

> From: Brad Templeton <brad%looking.uucp@RELAY.CS.NET>
> People are talking as though there's some
> surprising end-of-the-world potential in this event...
> University systems are designed, and should be designed as
> low-caution, high convenience systems... The press
> will want sensationalistic answers, but if you're talking to
> them, try to steer them away from all the comments about
> "War Games."

I was interviewed specifically on whether the worm illustrated a potential cause of nuclear Armageddon. (Bay Area TV Channel 7 (ABC), 11pm news Nov.4, lead story.) My answer was a qualified affirmative, and I think an unqualified negative irresponsible. Directly asked whether "War Games" was a good analogy, I responded that things were generally headed that way but that the Vincennes shootdown was a closer analogy to the present parlous state. (The Pentagon having concluded that no person was at fault for the mistaken shootdown, the cause was by default computer-related error.)

In some circumstances, a computer virus/worm could be a determinative factor precipitating a nuclear strike. Nuclear command and control computerization involves two functionally distinct sets of systems: (a) those for *executing* a nuclear attack a la SIOP recipes; (b) those for *prompting* a strike by informing the military (or political) leaders that an attack should be launched, which includes notice of (predefined) preemptive and launch on warning contingencies.

Execute command systems could be relatively closed; and hence are, or could be managed so as to be, relatively secure. Nevertheless, it gives pause that the system requires that underground officers respond immediately if valid launch codes are suddenly received through electronic communication channels. Note well that message traffic processed in the launch control capsules has greatly increased in recent years.

Re the strategic and tactical warning systems, they are already based on networked/workstation systems, i.e. the IDHS (Intelligence Data Handling System), and DEFSMAC, which link the CIA, NSA, DIA, JCS, NORAD, and SIOP-CINCS. These are of the same ilk as Arpanet/Milnet, and access is very wide, albeit not public. Intelligence-gathering/data-fusion by its function requires a network open to diverse and disparate inputs, and so is vulnerable to

disruption/confusion by viruses/worms et alia. While such systems may be impervious to telenet attack, and while published "bugs" like the UNIX debug option may be foreclosed in them, the potential for implanting subtle bugs/traps in the software is plain, and that is but one potential source of error. Infiltration of software companies/military programming seems easy and suggests *real* espionage possibilities that are frightening in their scope and mulitplicity. Also frightening is that the apparent failure of nodes in the tactical warning net is interpreted as notice that those nodes may have been destroyed in a nuclear attack. (NORAD and other testimony admits this.) There is manifestly the potential for accidental/malicious net malfunctions causing a catastrophic nuclear panic.

As for the trends, despite first appearances, the "Star Wars" system would greatly add to U.S. vulnerability rather than to security by resting U.S. strategic execution (as well as warning) upon a huge network of systems, much harder to secure than the present execution system. The warning system also becomes much more complex. The funded National Test Bed is in essence the development of such vulnerable networks for strategic warning and execution.

The pace of technology is not the *imperative* that the military claim must be followed so as to sustain deterrence. The probable futility of plugging holes in vast computer networks is at least as vital a message as the message that known holes can be effectively patched. The fact that the military widely use complex networks in nuclear planning means that a most urgent lesson is that we must avoid critical reliance on them, not merely that we should carry on under the placebo of plugging what holes are identified.

The Worm

Vince Manis <manis@grads.cs.ubc.ca>
Mon, 7 Nov 88 07:56:14 PST

Our site apparently didn't get hit, because our newly installed NSFnet router has been so flaky that it has been unusable. Just goes to show, I guess.

I was struck by the fact that the biggest hole was the `debug' option in sendmail. Since it has been well-known for about 15 years that allowing anonymous remote execution is a tremendous danger, and since (I assume) sendmail, in the standard distribution, comes with it disabled, one has to ask why SA's were enabling it. I'm not entirely sure that all the blame should go to the worm's author (putatively Mr Morris).

If the assumption in the previous paragraph is false, then perhaps UCB, Sun, and Mt Xinu (among others) are at least morally culpable, too.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 74

Thursday 10 November 1988

Contents

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

Air traffic control and safety margins

Steve Philipson <steve@aurora.arc.nasa.gov>
Wed, 9 Nov 88 12:19:13 PST

In rISKS-7.72, Jeffrey Mogul, Computer science unencumbered by fears about cutting safety margins, submitted some quotes from "Airport" magazine":

> Aviation Scientists in Britain, the US, France and West Germany are
> now working on a data-exchange system which would reduce or even
> eliminate the human element in air traffic control and in airport
> approach, landing and take-off-slot technique.

I'm not sure what "approach, landing and take-off-slot technique" means (this is not an expression in use in the field), but I can tell you that many of us in the field do not see terminal area control being handled by computer control in the forseeable future. The "human element" provides levels of redundancy, error checking, and distributed reasonablness checks that would likely be lost in a computer controlled system.

> Machine-talking-to-machine would enable the system to improve
> perhaps five-fold, because the precise nature of computer science
> is unencumbered by fears about cutting safety margins too finely. A
> cold dish of comfort, perhaps; one which will not be available until
> well after 2005. And anyway, nobody knows yet how much such a system
> will cost. But we all know who's going to pay for it, don't we?

One of the most significant losses in such a system is the loss of the "party line". Each flight crew hears the ATC instructions issued to other aircraft on the frequency (and in their general area), and can recognize instructions that put two aircraft in conflict. We may never have a system where an aircraft is cleared for takeoff by computer, where other aircraft would not be aware of the issuance of that clearance. A ground computer to single aircraft computer system would DECREASE safety, as flight crews would lose the knowledge of the "big picture", i.e., what other aircraft are being told to do, and what the general flow of traffic is. (It is of tremendos import to know that another aircraft has been cleared for takeoff while you are taxiing on the same runway.) There are also substantial questions on the viability of text-based (as opposed to human voice based) communications with the attendant transfer from auditory to visual task loads and it's impact on visual traffic scan duties.

The author of the article seems to believe that computer systems are inherently more reliable and efficient than human systems, so we can solve our congestion and safety problems in one fell swoop just by using computer systems. RISKS readers recognize the falicy of that position, as do aviation safety researchers. On the other hand, he also seems to believe that the computer system will be terribly expensive. and that we'll be paying more even though we see a "five-fold" improvement in capacity. Sounds like a technically naive writer to me.

Steve Philipson

UK vehicle-identification systems

<"chaz_heritage.WGC1RX"@Xerox.COM>
9 Nov 88 11:21:15 PST (Wednesday)

In his Fri, 4 Nov 88 01:43:49 PST RISKS-7.72 contribution Dave Robinson writes:

> Last night, no BBC's TOP GEAR programme, a device deliberately designed to locate cars was described.
Essentially, it is a navigational aid designed to take into account traffic congestion.<

What Mr. Robinson did not mention (though it has been given scant treatment by the UK media) was the scheme for 'privatising' roads. This is part of the general policy of the UK Government that as little as possible of the national infrastructure should be publicly owned.

Though not necessarily all roads would immediately be sold off to speculators, the majority of tunnels, bridges and newly-constructed roads would, were the necessary legislation to be passed, become, or remain, privately owned.

The Government feel that the present method of collecting tolls is antiquated and causes congestion at vital points such as the Dartford Tunnel. They therefore have conceived an automatic toll-collection method, based, they say, on Japanese practice.

Every vehicle in the country would have to be fitted with what is described as an 'electronic number-plate'. Descriptions of this equipment are few, vague and couched in the usual patronising 'you-couldn't-possibly-understand-this' terms. However, its principle appears to be that of IFF (Identification: Friend or Foe?).

When the IFF-equipped vehicle is driven through a toll point, its IFF is interrogated by devices installed in the road surface. It then transmits, by some means, the vehicle's registration number to the interrogation devices. These communicate directly with the road owner's computer system. Clearly this computer system must either be connected to, or share a common database with, the Driver and Vehicle Licensing Centre at Swansea, which holds all records of registered vehicles. This would allow the road owner to bill drivers automatically. The Government claim (as they are wont to do in such cases) that this is 'what the majority of people want'. There has, of course, been no suggestion that the interrogation devices might also be connected to the Police National Computer, since such a suggestion would be either what the Government call 'irresponsible journalism' (if it were not demonstrably true) or a breach of the Official Secrets Acts (if it were). However, were I a senior Police Officer, I would find it difficult to refuse such an opportunity for what is fashionably described as 'pre-emptive policing'.

It would, of course, have to be made a crime to drive without an IFF device, or with a faulty one (how one is supposed to establish that one's IFF is working correctly - when its principle of operation is apparently a secret - is not clear).

It is curious that the Government, ostensibly anxious to allow maximum commercial freedom, should on the one hand declare their intention of selling off the roads to private investors, and on the other hand prepare to prescribe for those investors a national system of automatic vehicle identification. Were I the owner of a road or bridge I should resent being told by the Government that I had to use a particular, Government-prescribed toll system (tollbooths still work, and they're cheap!). One could almost draw the conclusion that something other than commercial efficiency had prompted the Government's decisions in this respect.

However, there cannot possibly be RISKS in this system, since, on the few occasions when it is publicly mentioned, there is always a qualifying assurance to the effect that 'the innocent have nothing to fear'. Why such assurances should have to be made in connection with an automatic toll system - totally unconnected, of course, with the security forces - is not clear.

Chaz

---

re: NYT/Markoff: The Computer Jam -- How it came about

Mark W. Eichin <eichin@ATHENA.MIT.EDU>
Wed, 9 Nov 88 19:58:41 EST

The following paragraph from Markoff's article comes from a telephone conversation he had with me at the airport leaving the Nov. 8 "virus conference":

> But Morris reasoned that another expert could defeat his program by sending
>the correct answering signal back to the rogue. To parry this, Morris
>programmed his invader so that once every 10 times it sent the query signal it
>would copy itself into the new machine regardless of the answer.
> The choice of 1 in 10 proved disastrous because it was far too frequent. It
>should have been one in 1,000 or even one in 10,000 for the invader to escape
>detection.

However, it is incorrect (I did think Markoff had grasped my comments, perhaps not.) The virus design seems to have been to reinfect with a 1 in 15 chance a machine already infected.

The code was BACKWARD, so it reinfected with a *14* in 15 chance. Changing the denominator would have had no effect.

Mark Eichin <eichin@athena.mit.edu> SIPB Member & Project Athena "Watchmaker"

The worm and the debug option

smb@research.att.com <Steven Bellovin> <hector!smb>
Wed, 9 Nov 88 23:01:29 EST

Sorry -- in both Berkeley's and Sun's standard distribution, debugging comes enabled. That's perhaps defensible from Berkeley; they're distributing a research system, to customers prone to tinker, and sendmail is certainly complex enough to need lot's of debugging. Nor can I necessarily criticize it from Sun; it's often useful to be able to trace such a program. The flaw is not that debug mode was possible; rather, that sendmail's debug mode (a) was accessible remotely; and (b) expanded the range of inputs accepted by the program, rather than just providing extra trace data. What's even more amazing is the statement Eric Allman (the author of sendmail) was quoted in the N.Y. Times as making: that he added that code to get around restrictive management policies. That is, it was a deliberate back door, albeit one with a nominally-limited intended scope. 10-Nov-88

Risks of unchecked input in C programs

<geoff@utstat.UUCP>
Thu 10 Nov EST 1988 03:13:37

A security bug in the 4.2BSD Unix finger daemon, which permitted its invoker to obtain a shell with super-user privileges, was exposed during the recent Internet worm discussion. The bug was caused by use of the C standard I/O routine "gets" which is a bug waiting to happen and which should be stamped out. (I have deleted gets from my standard I/O implementation, and the folks at Bell Labs Research have deleted gets from their C library.) The bug was that the finger daemon used gets to read a line of input from its network connection, and gets is unable to check that the input line fits within the buffer handed to gets, so a suitably-constructed line of input to the finger daemon steps on other variables, confusing the finger daemon.

gets, as part of standard I/O, is a decade-old backward-compatibility hack for compatibility with the Sixth Edition UNIX Portable I/O Library, which was utterly replaced by standard I/O no later than 1979. gets takes one parameter, the input buffer into which a line of input from the standard input stream is to be stored, and deletes any trailing newline from the buffer. Standard I/O contains an alternative to gets, called fgets, which takes three parameters: an input buffer, its size in bytes, and the stream to be read. fgets does not strip trailing newlines. Converting programs from using gets to fgets is largely mechanical, and stripping trailing newlines is trivial to code yourself. gets is inherently unsafe due to its inability to check for overrun of the buffer provided to it. There is no reason to use gets, and there are good reasons to avoid gets.

Geoff Collyer utzoo!utstat!geoff, geoff@utstat.toronto.edu

Worms/viruses/moles/etc. and the risks

Scott E. Preece <preece@xenurus.gould.com>
Thu, 10 Nov 88 09:38:49 CST

From: "Clifford Johnson" <GA.CJJ@Forsythe.Stanford.EDU>
> As for the trends, despite first appearances, the "Star Wars" system
> would greatly add to U.S. vulnerability rather than to security by
> resting U.S. strategic execution (as well as warning) upon a huge
> network of systems, much harder to secure than the present execution
> system. The warning system also becomes much more complex. The funded
> National Test Bed is in essence the
> development of such vulnerable networks for strategic warning and execution.

It's also interesting to note that many of the people defending the security of the "really" secure systems pointed to their reliance on physical security -- the lack of network or remote access. SDI, on the other hand, is going to depend on space-based components which CANNOT be isolated from remote access.

scott preece, motorola urbana design center
uucp: uunet!uiucuxc!mcdurb!preece

Nonsecure passwords/computer ethics

Christine Piatko <piatko@svax.cs.cornell.edu>
Wed, 9 Nov 88 15:56:43 EST

I would like to point out that the users themselves can make their passwords more secure by not using `obvious' (i.e. English word, easily available in the dictionary) passwords. At the moment it is too easy to encrypt dictionary entries and compare them to password files. People are told this all the time, but there are many people who use words that can be found in the dictionary. I'm sure the situation is similar at other sites (even for root passwords). People pick WORDS because they are easy to remember. A better technique, to come up with safer password, is to pick a phrase and use the initial letters and numbers:

'A stitch in time saves nine' for the password asits9.

Perhaps a program should be run every so often to check if people have obvious passwords and remind them to change them. If the message is ignored the user could be inconvenienced by having the administrator change the password for him.

Of course this does not address other issues, like the 'bug' in sendmail (which seemed more like a door that someone left open for himself) or other issues of system security. But this is one measure that users can take to protect themselves a bit.

In defense of the alleged culprit R. Morris, I would like to say that I know of people at several universities who have had similar escapades, although on a smaller scale. In this case I agree that the 'prank' got out of hand, but there are many such pranks going all the time at any system site. For some reason these kinds of holes are fascinating to some pretty intelligent people. I think their fascination should be put to good use tracking down such holes. I don't hold out much hope for completely secure systems (I don't believe there are break-in proof safes or unsinkable ships either). However this should emphasize the fact that we are a community that has to work together, and sometimes that means learning some very hard lessons together. If just one site had been affected, would the sendmail bug have been fixed nationwide? Evidently not, since from what I've seen on the net this bug was known about for at least 2 years.

As a community we have a lot to learn about how to work together. It is interesting to see so many different perspectives on how 'secure' computers and networks should be. I have been amused by people saying that we should require CS students to take an ethics course. Is it really so clear in the entire community what is and isn't ethical behavior? Obviously not, since some people think this 'worm' incident was merely stupid, while others think it was unethical. We in the computer science community need to figure out a code of ethics dealing with breaking into systems, just as we as a society are still figuring out how to deal with people who break into our homes.

Christine Piatko
usual disclaimers here, and no, I didn't know rtm very well.

Re: Nonsecure passwords/computer ethics

Peter G. Neumann <Neumann@KL.SRI.COM>
Wed, 9 Nov 88 13:09:18 PST

But don't forget that passwords traversing Ethernets and Arpanets are vulnerable even if they are difficult to guess. The net communications are unencrypted and capturable. Many years ago someone wrote a simple ID-and-password capture program on the Ethernet. It still works. In UNIX, the /dev/mem vulnerability (a "feature" to some) can be used to capture passwords in unencrypted form. Even the Gould UTX/32S C2 version of Unix still has that vulnerability. The bottom line is this: beware of relying on passwords. By the way, for Unix folks, the AT&T and Sun announcements of vastly improved security (including multilevel security) should be of considerable interest. But they still don't solve all the problems.

> [Ironically, perhaps, it is the classical paper by Bob Morris (Sr.) and Ken Thompson, "UNIX Password Security: A Case History", Comm. ACM 22, 11 (November 1979), pp. 594-597, that really started the increased awareness about password vulnerabilities!]

Phone-answerer/ voicemail security & voice-encryption

"David A. Honig" <honig@bonnie.ICS.UCI.EDU>
Wed, 09 Nov 88 13:42:33 -0800

Unauthorized phone-answering-machine playback and unauthorized centralized-voicemail message playback could be made more difficult by encrypting the stored messages. This could be done at the same time as data compression preprocessing on digital systems. (There are analog "encryption" methods but these days everything's cheaper digitally...)

Of course, the original message could be bugged when recorded, and for a central-voicemail system the encryption key would have to be sent over the (unsecure) phone lines, so this is not a total solution. But it makes it harder for nosy voicemail sysops, including those with warrants, to playback stored messages. And it makes unauthorized home-answering machine playback useless.

Encrypted voicemail and a more secure home answering machine most likely *are* good selling points, so I will not be too surprised when they become commercial. Some of the (e.g., black) market desires these features now, and when it becomes cheap, everyone will expect it.

University computing (Re: RISKS-7.71)

<"James_A._Schweitzer.STHQ"@Xerox.COM>
Thu, 10 Nov 88 10:23:19 PST

Peter, re: your comment that "But to assume that university computing should be relatively wide open would be a serious mistake. Unethical and other abuses are not uncommon."(Sun, 6 Nov 88 22:01:17 PST).

At a professional meeting last week, we had a presentation by a university data center manager on a Trojan Horse attack which had shut down his operation. The last part of his talk was titled "Lessons Learned". I was dumbfounded that these "lessons" included only technical conclusions concerning security controls. There was no thought of teaching the student users about computer ethics and proper behavior once you are granted computer use privileges.

I told him I though it was similar to teaching a fifteen-year-old to drive a car while neglecting to say anything about rules of the road, traffic signals, and so forth.

Until the universities start telling people about proper behavior, they (and I guess we) deserve what we get.

Jim Schweitzer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 75

Friday 11 November 1988

Contents

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

Re: Risks of unchecked input in C programs

<bobf@lotus.UUCP>
Fri Nov 11 14:35:06 1988

The point about "gets" having no way to assure that the supplied buffer is sufficient is a serious deficiency through the current ANSI(!) C library in routines such as sprintfv and strcpy. This is a sloppiness that might be justifiable in a hacking environment but is very dangerous and inexcusable for production programs. I find it amazing that such interfaces persist into product applications since what we have is an underspecified interface to important system functions.

Of course, one could avoid using this part of the C library, but writing safe code shouldn't be a matter of fighting the system, rather it should be an

expected use of the library.

Sorry if I seem so adamant about this but I've got to worry about supplying complex software to millions of users who are quite inventive in novel ways to (ab)use the software.

Bob Frankston

NY Computer Laws and the Internet Worm

Dave Bozak <dab@oswego.Oswego.EDU>
Fri, 11 Nov 88 11:23:17 est

In regards to the recent Internet Worm, I am amazed that the newspapers continually report that the FBI is not sure that any laws were broken. In New York State, as of November 1, 1987, the penal law was amended to include a new article, 156, titled "Offenses Involving Computers". There are 2 relevant offenses.

Section 156.05: Unauthorized use of a computer. A person is guilty of unauthorized use of a computer when he knowingly uses or causes to be used a computer or computer service without authorization and the computer utilized is equipped or programmed with any device or coding system, a function of which is to prevent the unauthorized use of said computer or computer system. Unauthorized us of a computer is a class A misdemeanor.

Section 156.10: Computer trespass. A person is guilty of computer trespass when he knowingly uses or causes to be used a computer or computer service without authorization and: 1. he does so with of any felony; or 2. he thereby knowingly gains access to computer material. Computer trespass is a class E felony.

Clearly the design and release of a worm is a violation of section 156.10. The worm was released was intended to gain access to machines without authorization and was designed to gain access to material (host lists) for propagation of the worm.

A felony is defined as an offense for which a sentence to a term of imprisonment in excess of one year is authorized in the state.

Now maybe I am missing something here, not being a lawyer...so would learned colleagues please clarify the legal issues involved in this particular case?

Ethics

<Stahl@DOCKMASTER.ARPA>
Fri, 11 Nov 88 00:51 EST

It's interesting that after the generally in-synch technical discussions re RTM's virus, unanimity breaks down when the subject turns to ethics.

Christine Piatko, on the one hand, questions whether we can define computer ethics in the absence even of agreement over house break-ins. Jim Schweitzer, on the other hand, suggests that there ought not be any question about proper computer ethics; that computer ethics is not

dissimilar to traffic rules.

I suggest that the situation is both less complicated than Piatko suggests and more so than Schweitzer does. As for Piatko, I would hope that as a society we agree that it is wrong to break into someone else's home and, that whatever disagreement we might have, it is over the punishment not the crime. Schweitzer, I believe, risks trivializing significant ethical issues because, when all is said and done, traffic rules have nothing to do with ethics but are agreed upon protocols for sharing roadways.

The critical bottom line, and it is one that shouts out to us in the wake of the RTM worm, is that we absolutely must begin to take the teaching of ethics seriously. Some school districts are beginning to do this and they are to be commended for it. Perhaps if everyone were exposed to ethics courses, beginning in the early grades and continuing through computer ethics courses and business ethics courses, etc, then it would be clear `in the entire community what is and what isn't ethical behavior.'

Stan Stahl

Re: insecure passwords/computer ethics

Christine Piatko <piatko@svax.cs.cornell.edu>
Fri, 11 Nov 88 11:37:38 EST

I forgot about electronic snooping. I was mostly thinking of the 'common password list' that was found with the virus. At least some of them were actual passwords of people at Cornell that were common English words.

I didn't realize the Ethernet was wide open for such snooping. Maybe that will happen next.

Christine

Comments sought on proposed computer ethics course

Bob Barger <CFRNB@ECNCDC.BITNET>
Fri 11 Nov 1988 11:45 CDT

Eastern Illinois University has a two-semester-hour requirement for senior year students of a seminar "organized around a particular subject/issue important to contemporary society" which must be taken in a field outside the student's major field of study. The following is a seminar proposal on which comments/suggestions are sollicited:
COMPUTER ETHICS: This seminar will investigate current ethical issues involving computers. There will be no class meetings, except for the first and last sessions. Students will instead utilize electronic bulletin boards on the university's mainframe computer network to research and discuss issues.
Week: Topic:

1 Orientation to the course: initially, the seminar members will meet as a group in a traditional class setting for purposes of introduction, and explanation of course content, ethical paradigms, class procedures, and evaluation criteria.

2-14 Weekly on-line reading of such bulletin boards as "Discussion of Ethics in Computing" (ETHICS L) and the "Forum on Risks to the Public in Computers and Related Systems" (RISKS), weekly posted reactions to these readings, and posted comments on other students' reactions.

15 Final examination and course evaluation: the seminar members will reconvene as a group for the last meeting to allow for individual examinations and group reflection on the seminar experience.

Writing component:

Students will compose a weekly 30-to-50 line reaction to their bulletin board readings. These reactions will be posted (i.e., sent to the mainframe computer bulletin board set aside for members of this seminar). In their reaction, 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 on which the author seems to be depending, 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 previous comments under #5 above. The instructor will send to the student, by electronic mail, a weekly grade on the student's posted reaction, together with whatever comments the instructor thinks helpful. The student's original posted reaction will be open to public comment by the other students in the seminar [this will be accomplished by posting notes to the bulletin board, referencing the original reaction]. These latter comments by the other students in the seminar will form the basis for the "participation" factor of the 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 posted comments on other students' reactions) = 20%
- Final Exam = 15%

Send comments to: Bob Barger<cfrnb@ecncdc.bitnet>.
Suggestions for texts in computer ethics are especially sollicited.

UK vehicle-identification systems

Douglas Jones <jones@herky.cs.uiowa.edu>
Thu, 10 Nov 88 18:06:52 CST

In his 9 Nov 88 11:21:15 PST RISKS contribution, Chaz Heritage suggested that the electronic number plates to be fitted on every vehicle were to be some kind of IFF (Identification: Friend or Foe) device. This suggests an active electronic transponder of some type. In fact, the technology needed for road vehicle identification is much simpler, comparable to the automatic car location technology used by the railroads. In the United States, we use a black rectangle painted on the side of each railroad car, on which colored tape has been fixed in a machine readable pattern. Bar code scanners located at the track side can read these as the train moves. (aside: the bar code is read vertically, so it remains readable independently of the direction of train motion, and there is a wide latitude in the allowed positions of the code.) The only problem with the US system is that the code has to be washed once in a while or it gets grime covered and unreadable.

In the UK, I heard about 15 years ago that they were experimenting with a microwave readable bar code for automatic car location. This was readable through arbitrary accumulations of grime, and was constructed of a metal channel with covers welded over the channel to give a binary code. Something like this, mounted on the underside of a car, would be quite practical for automatic road vehicle identification, with sensors reading from below as the car passes through the "toll station".

The risk of such sensors as police devices depends to a great extent on how easy it is to instrument locations in the roadway without the driver being aware of it. The grime-proof channel described above would be read from below, and a car would have to pass directly over the reader, so it wouldn't work on the open road, where cars could easily dodge the sensor. US style bar codes are easily covered, but when exposed, can be read from an inconspicuous roadside scanner. Aircraft style IFF devices would allow actual tracking of cars from a distance without fixed scanners.

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

---

UK vehicle-id systems... Big Brother's new eyes?

<hadj@sbcs.sunysb.edu>
Fri, 11 Nov 88 19:20:08 EST

In RISKS 7.74 "chaz_heritage.WGC1RX"@Xerox.COM writes:

>Every vehicle in the country would have to be fitted with what is described
>as an 'electronic number-plate'. ...

>When the IFF-equipped vehicle is driven through a toll point, its IFF is
>interrogated by devices installed in the road surface. It then transmits,
>by some means, the vehicle's registration number to the interrogation
>devices. These communicate directly with the road owner's computer system.
>Clearly this computer system must either be connected to, or share a common
>database with, the Driver and Vehicle Licensing Centre at Swansea, which
>holds all records of registered vehicles. ...

>... There has,
>of course, been no suggestion that the interrogation devices might also be
>connected to the Police National Computer, since such a suggestion would be
>either what the Government call 'irresponsible journalism' (if it were not
>demonstrably true) or a breach of the Official Secrets Acts (if it were). ...

>It would, of course, have to be made a crime to drive without an IFF
>device, or with a faulty one (how one is supposed to establish that one's
>IFF is working correctly - when its principle of operation is apparently a
>secret - is not clear).

I find this to be a terrifying bit of news, based on the fact that a
government will always use the information it can get access to, if
necessary...(if a court can get access to a reporter's notes, why not
a road owner's database?)

Possible uses:
1) the use of such travel information in a case against a suspected
criminal:
Lawyer: "Where were you on the night of Nov 8, 1988?"
Defendant:"I was sitting at home watching TV."
Lawyer: "Not true! Your car was observed passing toll
FOO on interstate BAR!"

2) the use of such information to find lawbreakers:
A trivial example: such information could be used to catch people
speeding on the highway. Attach a timestamp to each event and
calculate v = dx/dt.

There is, of course, nothing wrong with catching criminals. However,
the described system depends on privately owned computers and
various unreliable components (transmitters, etc) which are not
impervious to accidental or deliberate tampering. It seems easy
enough to fake evidence of this sort. Even if we assume the database
is 100% secure, the data collected could be corrupted. It seems
unlikely that the IFF boxes will be immune to reverse engineering.
Imagine a box that sends out a random ID signal every time it passes
though a toll point.

It is troublesome to think that somewhere, in some computer
database, there is a record of where and when some computer _thinks_
that i was detected driving my car.

The potential for invasion of privacy is enormous, and made more
frightening by the fallibility of the system. It is a powerful
system based on an insecure database. It would give Big Brother
one more set of eyes on the world.

-mike hadjimichael.

{ hadj@sbcs.sunysb.edu {philabs, allegra}!sbcs!hadj }
{ departmentofcomputersciencesunystonybrookstonybrooknyoneonesevenninefour }

Re: Phone-answerer/ voicemail security & voice-encryption

<jik@ATHENA.MIT.EDU>
Thu, 10 Nov 88 18:05:11 EST

> Date: Wed, 09 Nov 88 13:42:33 -0800
> From: "David A. Honig" <honig@bonnie.ICS.UCI.EDU>
>
> Unauthorized phone-answering-machine playback and unauthorized
> centralized-voicemail message playback could be made more difficult
> by encrypting the stored messages. This could be done at the same
> time as data compression preprocessing on digital systems. (There
> are analog "encryption" methods but these days everything's cheaper
> digitally...)

Yes, but the whole point is that the answering machines currently on the market provide minimal message security because the access codes are so ridiculously simple to "crack" (I place "crack" in quotes because I'm not sure the task is difficult enough to call it "cracking."). In order for encrypted-data answering machines to allow remote message access, they would expect you to enter the decryption key over the phone line. If the decryption key is complex enough that it cannot be guessed (which is really the question is being asked here), then why use encryption at all? Just use that key as the password, and security is assured (as much as it can be, at least).

In other words, I fail to see how data encryption provides an increased measure of security in the context of the problem we are discussing, which is the lack of a secure password.

Jonathan Kamens, Massachusetts Institute of Technology -- Project Athena

Re: Ultrasonic emissions a real problem

Travis Lee Winfrey <travis@douglass.cs.columbia.edu>
Fri, 11 Nov 88 15:36:34 EST

>Date: Mon, 07 Nov 88 18:13:29 EST
>From: Geoffrey Welsh <izot@f171.n221.z1.fidonet.org>
>Subject: Ultrasonic emissions a real problem
> What, then, leads some of us to be sensitive to these frequencies to a
>fault and others to be completely unaware of them? Worse, how can we determine
>what levels are acceptable, given that some people are simply more sensitive
>than others?

Although I don't know why, asthmatics are known to hear very high sound frequencies, well over 22 KHz. I've been able to hear terminals, TVs, dog whistles since I was very young. Brand X CRT's and Kaypro's have made me clap my hands to my ears.

> If indeed ultrasonic emissions are a cause of illness or other unacceptable
>consequences, it is vital that a study into the area be launched. Who knows;

>in a few years we may find our present CRTs replaced with ones that have a
>horizontal scan rate above 30 KHz to avoid this problem.

It was explained to me once. There is a common component in RGB CRT's which alternates very rapidly, around 26-28 KHz. Particularly in older TV's, this component takes a while to cycle up, which is why when someone turns on a TV in the next apartment (or building!), I can hear the high-pitched sound it makes begin loudly then almost disappear.

I personally would worry more about vision, back, and stress problems caused by introducing computers into the workplace. The high-pitched sounds falls more into the category of Stupid People Tricks.

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 76

Saturday 12 November 1988

Contents

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

Computer Literacy #2

Ronni Rosenberg <ronni@juicy-juice.lcs.mit.edu>
Wed, 9 Nov 88 16:43:58 EST

A typical computer-literacy course has the following components. What do you think of this operational description of computer literacy? Should other topics be taught instead? in addition to these? Should everyone study this? As before, send mail to RISKS or to me, depending on your preference.

1. TERMINOLOGY AND JARGON: This is designed to enable students to "talk knowledgeably" about computers. Here are some definitions of a computer, from computer-literacy textbooks:

* "A computer is an electronic machine that solves problems or answers questions.""
* "A computer ... is a machine that can handle large amounts of information and work with amazing speed."
* "A computer is an electronic tool that helps people do many different things faster, easier, or better."

Here is another definition, from a graduate computer-literacy class (for teachers, administrators, computer coordinators, and so on):

* "An operating system is a program that tells the computer how to deal with information -- tells it how to move information, how to operate, how to

do things. ... An operating system is done in a lower level language, machine language. It really controls the flow of electricity through the circuits."

2. HARDWARE: This is designed to give students a "working knowledge of computer equipment." Typical classes use Apple IIs. The last large surveys show a national average of 1 machine per 40 students (grades K-12). Many schools cannot afford two disk drives per machine. A computer lab of 10-30 machines might have 1-3 printers (dot matrix). Devices such as joysticks, mice, and touch-sensitive displays are too expensive for most schools to buy (or these devices operate on machines that are too expensive), but some schools buy one of each, to pass around a class. The emphasis is on identifying components and handling equipment (e.g., floppy disks). A 1988 survey showed that among 11th grade students:

* 30% did not know what a cursor does,
* 60% did not know what a modem does, and
* 40% could not identify a spreadsheet as a software component or a video display as a hardware component.

3. SOFTWARE: Exposure to "basic software concepts" is designed to enable students to use computers as tools and to "remove the mystery of computers." Typical classes show programs for word processing (which predominates), spreadsheets, and databases -- ones that run on Apple IIs (or, in many cases, smaller machines). Students do not see actual program documentation. The emphasis is on the syntax of program commands. The survey cited above showed that students scored

* 72% correct on word-processing questions
* 52% correct on spreadsheet questions
* 31% correct on database questions

4. PROGRAMMING: When included, this means BASIC or LOGO programming. Again, the emphasis is on learning the syntax of some language commands. Miniscule programs (e.g., 10 lines) predominate.

5. JOBS IN COMPUTING: When included, this means brief discussion of careers in computing. There is a widespread sense that "computer literacy" is the passport to well paying jobs.

6. SOCIAL IMPACTS OF COMPUTERS: When included, this encompasses computer uses, ethics, and legal implications. Under uses, students might be told, for instance, that the FBI uses computers to store data on criminals and crimes, but not about privacy risks, data quality problems, etc. Students might be told that some people lose jobs because of computer automation -- and that these people can get other jobs working with computers. Ethics means a mention of computer crime. Legal implications means a warning that students should not copy software disks they use in class. Students are explicitly encouraged to have "positive attitudes about computers." Topics not covered include whistleblowing, the military influence on the computer profession, limits of simulations, and risks of large computer systems.

(long) report on the Internet Worm

Ken van Wyk <luken@SPOT.CC.LEHIGH.EDU>
Fri, 11 Nov 88 13:57:42 EST

A REPORT ON THE INTERNET WORM

Bob Page
University of Lowell
Computer Science Department

November 7, 1988

Here's the scoop on the "Internet Worm". Actually it's not a virus - a virus is a piece of code that adds itself to other programs, including operating systems. It cannot run independently, but rather requires that its "host" program be run to activate it. As such, it has a clear analog to biologic viruses -- those viruses are not considered live, but they invade host cells and take them over, making them produce new viruses.

A worm is a program that can run by itself and can propagate a fully working version of itself to other machines. As such, what was loosed on the Internet was clearly a worm.

This data was collected through an emergency mailing list set up by Gene Spafford at Purdue University, for administrators of major Internet sites - some of the text is included verbatim from that list. Mail was heavy since the formation of the list; it continues to be on Monday afternoon - I get at least 2-3 messages every hour. It's possible that some of this information is incomplete, but I thought you'd like to know what I know so far.

The basic object of the worm is to get a shell on another machine so it can reproduce further. There are three ways it attacks: sendmail, fingerd, and rsh/rexec.

THE SENDMAIL ATTACK:

In the sendmail attack, the worm opens a TCP connection to another machine's sendmail (the SMTP port), invokes debug mode, and sends a RCPT TO that requests its data be piped through a shell. That data, a shell script (first-stage bootstrap) creates a temporary second-stage bootstrap file called x$$,l1.c (where '$$' is the current process ID). This is a small (40-line) C program.

The first-stage bootstrap compiles this program with the local cc and

executes it with arguments giving the Internet hostid/socket/password of where it just came from. The second-stage bootstrap (the compiled C program) sucks over two object files, x$$,vax.o and x$$,sun3.o from the attacking host. It has an array for 20 file names (presumably for 20 different machines), but only two (vax and sun) were compiled in to this code. It then figures out whether it's running under BSD or SunOS and links the appropriate file against the C library to produce an executable program called /usr/tmp/sh - so it looks like the Bourne shell to anyone who looked there.

THE FINGERD ATTACK:

In the fingerd attack, it tries to infiltrate systems via a bug in fingerd, the finger daemon. Apparently this is where most of its success was (not in sendmail, as was originally reported). When fingerd is connected to, it reads its arguments from a pipe, but doesn't limit how much it reads. If it reads more than the internal 512-byte buffer allowed, it writes past the end of its stack. After the stack is a command to be executed ("/usr/ucb/finger") that actually does the work. On a VAX, the worm knew how much further from the stack it had to clobber to get to this command, which it replaced with the command "/bin/sh" (the bourne shell). So instead of the finger command being executed, a shell was started with no arguments. Since this is run in the context of the finger daemon, stdin and stdout are connected to the network socket, and all the files were sucked over just like the shell that sendmail provided.

THE RSH/REXEC ATTACK:

The third way it tried to get into systems was via the .rhosts and /etc/hosts.equiv files to determine 'trusted' hosts where it might be able to migrate to. To use the .rhosts feature, it needed to actually get into people's accounts - since the worm was not running as root (it was running as daemon) it had to figure out people's passwords. To do this, it went through the /etc/passwd file, trying to guess passwords. It tried combinations of: the username, the last, first, last+first, nick names (from the GECOS field), and a list of special "popular" passwords:

aaa	cornelius	guntis	noxious	simon
academia	couscous	hacker	nutrition	simple
aerobics	creation	hamlet	nyquist	singer
airplane	creosote	handily	oceanography	single
albany	cretin	happening	ocelot	smile
albatross	daemon	harmony	olivetti	smiles
albert	dancer	harold	olivia	smooch
alex	daniel	harvey	oracle	smother
alexander	danny	hebrides	orca	snatch
algebra	dave	heinlein	orwell	snoopy
aliases	december	hello	osiris	soap
alphabet	defoe	help	outlaw	socrates
ama	deluge	herbert	oxford	sossina

amorphous desperate hiawatha pacific sparrows
analog develop hibernia painless spit
anchor dieter honey pakistan spring
andromache digital horse pam springer
animals discovery horus papers squires
answer disney hutchins password strangle
anthropogenic dog imbroglio patricia stratford
anvils drought imperial penguin stuttgart
anything duncan include peoria subway
aria eager ingres percolate success
ariadne easier inna persimmon summer
arrow edges innocuous persona super
arthur edinburgh irishman pete superstage
athena edwin isis peter support
atmosphere edwina japan philip supported
aztecs egghead jessica phoenix surfer
azure eiderdown jester pierre suzanne
bacchus eileen jixian pizza swearer
bailey einstein johnny plover symmetry
banana elephant joseph plymouth tangerine
bananas elizabeth joshua polynomial tape
bandit ellen judith pondering target
banks emerald juggle pork tarragon
barber engine julia poster taylor
baritone engineer kathleen praise telephone
bass enterprise kermit precious temptation
bassoon enzyme kernel prelude thailand
batman ersatz kirkland prince tiger
beater establish knight princeton toggle
beauty estate ladle protect tomato
beethoven euclid lambda protozoa topography
beloved evelyn lamination pumpkin tortoise
benz extension larkin puneet toyota
beowulf fairway larry puppet trails
berkeley felicia lazarus rabbit trivial
berliner fender lebesgue rachmaninoff trombone
beryl fermat lee rainbow tubas
beverly fidelity leland raindrop tuttle
bicameral finite leroy raleigh umesh
bob fishers lewis random unhappy
brenda flakes light rascal unicorn
brian float lisa really unknown
bridget flower louis rebecca urchin
broadway flowers lynne remote utility
bumbling foolproof macintosh rick vasant
burgess football mack ripple vertigo
campanile foresight maggot robotics vicky
cantor format magic rochester village
cardinal forsythe malcolm rolex virginia
carmen fourier mark romano warren
carolina fred markus ronald water
caroline friend marty rosebud weenie
cascades frighten marvin rosemary whatnot

castle fun master roses whiting
cat fungible maurice ruben whitney
cayuga gabriel mellon rules will
celtics gardner merlin ruth william
cerulean garfield mets sal williamsburg
change gauss michael saxon willie
charles george michelle scamper winston
charming gertrude mike scheme wisconsin
charon ginger minimum scott wizard
chester glacier minsky scotty wombat
cigar gnu moguls secret woodwind
classic golfer moose sensor wormwood
clusters gorgeous morley serenity yaco
coffee gorges mozart sharks yang
coke gosling nancy sharon yellowstone
collins gouge napoleon sheffield yosemite
commrades graham nepenthe sheldon zap
computer gryphon ness shiva zimmerman
condo guest network shivers
cookie guitar newton shuttle
cooper gumption next signature

[I wouldn't have picked some of these as "popular" passwords, but then again, I'm not a worm writer. What do I know?]

When everything else fails, it opens /usr/dict/words and tries every word in the dictionary. It is pretty successful in finding passwords, as most people don't choose them very well. Once it gets into someone's account, it looks for a .rhosts file and does an 'rsh' and/or 'rexec' to another host, it sucks over the necessary files into /usr/tmp and runs /usr/tmp/sh to start all over again.

Between these three methods of attack (sendmail, fingerd, .rhosts) it was able to spread very quickly.

THE WORM ITSELF:

The 'sh' program is the actual worm. When it starts up it clobbers its argv array so a 'ps' will not show its name. It opens all its necessary files, then unlinks (deletes) them so they can't be found (since it has them open, however, it can still access the contents). It then tries to infect as many other hosts as possible - when it sucessfully connects to one host, it forks a child to continue the infection while the parent keeps on trying new hosts.

One of the things it does before it attacks a host is connect to the telnet port and immediately close it. Thus, "telnetd: ttloop: peer died" in /usr/adm/messages means the worm attempted an attack.

The worm's role in life is to reproduce - nothing more. To do that it needs to find other hosts. It does a 'netstat -r -n' to find local routes to other hosts & networks, looks in /etc/hosts, and uses the

yellow pages distributed hosts file if it's available. Any time it finds a host, it tries to infect it through one of the three methods, see above. Once it finds a local network (like 129.63.nn.nn for ulowell) it sequentially tries every address in that range.

If the system crashes or is rebooted, most system boot procedures clear /tmp and /usr/tmp as a matter of course, erasing any evidence. However, sendmail log files show mail coming in from user /dev/null for user /bin/sed, which is a tipoff that the worm entered.

Each time the worm is started, there is a 1/15 chance (it calls random()) that it sends a single byte to ernie.berkeley.edu on some magic port, apparently to act as some kind of monitoring mechanism.

THE CRACKDOWN:

Three main 'swat' teams from Berkeley, MIT and Purdue found copies of the VAX code (the .o files had all the symbols intact with somewhat meaningful names) and disassembled it into about 3000 lines of C. The BSD development team poked fun at the code, even going so far to point out bugs in the code and supplying source patches for it! They have not released the actual source code, however, and refuse to do so. That could change - there are a number of people who want to see the code.

Portions of the code appear incomplete, as if the program development was not yet finished. For example, it knows the offset needed to break the BSD fingerd, but doesn't know the correct offset for Sun's fingerd (which causes it to dump core); it also doesn't erase its tracks as cleverly as it might; and so on.

The worm uses a variable called 'pleasequit' but doesn't correctly initialize it, so some folks added a module called _worm.o to the C library, which is produced from:

```
int pleasequit = -1;
```

the fact that this value is set to -1 will cause it to exit after one iteration.

The close scrutiny of the code also turned up comments on the programmer's style. Verbatim from someone at MIT:

> From disassembling the code, it looks like the programmer is really anally retentive about checking return codes, and, in addition, prefers to use array indexing instead of pointers to walk through arrays.

Anyone who looks at the binary will not see any embedded strings - they are XOR'ed with 81 (hex). That's how the shell commands are imbedded. The "obvious" passwords are stored with their high bit set.

Although it spreads very fast, it is somewhat slowed down by the fact that it drives the load average up on the machine - this is due to all the encryptions going on, and the large number of incoming worms from

other machines.

[Initially, the fastest defense against the worm is is to create a directory called /usr/tmp/sh. The script that creates /usr/tmp/sh from one of the .o files checks to see if /usr/tmp/sh exists, but not to see if it's a directory. This fix is known as 'the condom'.]

NOW WHAT?

None of the ULowell machines were hit by the worm. When BBN staffers found their systems infected, they cut themselves off from all other hosts. Since our connection to the Internet is through BBN, we were cut off as well. Before we were cut off, I received mail about the sendmail problem and installed a patch to disable the feature the worm uses to get in through sendmail. I had made local modifications to fingerd which changed the offsets, so any attempt to scribble over the stack would probably have ended up in a core dump.

Most Internet systems running 4.3BSD or SunOS have installed the necessary patches to close the holes and have rejoined the Internet. As you would expect, there is a renewed interest in system/network security, finding and plugging holes, and speculation over what will happen to the worm's creator.

If you haven't read or watched the news, various log files have named the responsible person as Robert Morris Jr., a 23-year old doctoral student at Cornell. His father is head of the National Computer Security Center, the NSA's public effort in computer security, and has lectured widely on security aspects of UNIX.

Associates of the student claim the worm was a 'mistake' - that he intended to unleash it but it was not supposed to move so quickly or spread so much. His goal (from what I understand) was to have a program 'live' within the Internet. If the reports that he intended it to spread slowly are true, then it's possible that the bytes sent to ernie.berkeley.edu were intended to monitor the spread of the worm. Some news reports mentioned that he panicked when, via some "monitoring mechanism" he saw how fast it had propagated.

A source inside DEC reports that although the worm didn't make much progress there, it was sighted on several machines that wouldn't be on its normal propagation path, i.e. not gateways and not on the same subnet. These machines are not reachable from the outside. Morris was a summer intern at DEC in '87. He might have included names or addresses he remembered as targets for infesting hidden internal networks. Most of the DEC machines in question belong to the group he worked in.

The final word has not been written - I don't think the FBI have even met with this guy yet. It will be interesting to see what happens.

NSA attempts to restrict virus information

<jon@june.cs.washington.edu>
Fri, 11 Nov 88 18:56:45 PST

The following excerpts are from THE NEW YORK TIMES, Nov 11 1988 p. 12:

US IS MOVING TO RESTRICT ACCESS TO FACTS ABOUT COMPUTER VIRUS by John Markoff

Government officials are moving to bar wider dissemination of information on techniques used in a rogue software program that jammed more than 6,000 computers in a nationwide computer network last week.

Their action comes amid bitter debate among computer scientists ... One group of experts believes wide publication of such information would permit computer network experts to identify problems more quickly and to correct flaws in their systems. But others argue that such information is too potentially explosive to be widely circulated.

Yesterday, officials at the National Computer Security Center, a division of the National Security Agency, contacted researchers at Purdue University in West Lafayette, Ind., and asked them to remove information from campus computers describing internal workings of the software program that jammed computers around the nation on Nov. 3. ... (A spokesperson) said the agency was concerned because it was not certain that all computer sites had corrected the software problems that permitted the program to invade systems in the first place. ...

Some computer security experts said they were concerned that techniques developed in the program would be widely exploited by those trying to break into computer systems. ...

- Jonathan Jacky, University of Washington

Who is responsible for the sendmail fiasco?

<bobf@lotus.UUCP>
Wed Nov 9 01:42:09 1988

The lesson from the PC world is that we can assign official responsibility to the system administrators but in practice they should not be expected to have the expertise. The expertise lies with those distributing turnkey workstation systems. Sun? Berkeley??

Bob Frankston

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 77

Monday 14 November 1988

Contents

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

UNIX InSecurity (beyond the Virus-Worm)

Klaus Brunnstein <brunnstein%rz.informatik.uni-hamburg.dbp.de@RELAY.CS.NET>
11 Nov 88 15:27 GMT+0100

Sitting far away from the `center of epidemy' (and not using UNIX), I observe with great interest the analysis of the `Virus Worm'. In FRG newsmedia, the New York Times article produced public uproar, with several

newspapers and the magazine `Der SPIEGEL' (in its November 7 edition) speculating, that something similar might happen to the computers of banks, tax authorities and state agencies. Moreover, the damage is reported to have affected `more than 6.000 large computers connected to ARPANET', and additionally, Joseph Weizenbaum is cited saying that this virus may also affect the really sensitive military US-installations.

Evidently, a large portion of the newsproducers is infected by the `Virus of Disinformation'. First lesson to be learned: the insecurity of relevant operating systems, well-known to experts since long time, must be disseminated from specialists to the computer profession. If even Edp people are not conscious of the risks imbedded in today's operating systems, we cannot hope for solid public presentation of such events.

In my personal fight against usage of UNIX in processing sensitive data (such as in medical, economical and public applications), I usually find my audience deeply surprised when citing F.T.Grampp and R.H.Morris, who in their AT&T Bell Lab Technical Journal (October 1984) article about UNIX Operating System Security wrote, after analysing the merits of `open systems' such as UNIX:

> `Such open systems cannot ever be made secure in any strong sense; that is, they are unfit for applications involving classified government information, corporate accounting, records relating to individual provacy, and the like...'

When I chaired, at the German Unix User Group annual conference in Hannover, September 1988, the session devoted to UNIX SECURITY, one speaker analysed that a Secure UNIX would hardly get a higher Orange Book classification than C2 or B1 because otherwise the restrictions and changes would produce something very different. A `security shell', as now planned by X/OPEN, is a contradiction in itself, because effective security must be implemented in the kernel. Moreover, real security deficiencies are even worse, as `most UNIX systems are far less secure than they can and should be', as Grampp/Morris wrote in 1984: while the SENDMAIL/DEBUG allows for worm applications such as network and remote system monitoring, fault analysis and maintenance, it may be the basis of even really harmful crimoid applications, such as Trojan Horses, Viruses or automated espionage programs.

(While Gould hopes to get DoD class B1, sometime early in 1989, for its new Secure UNIX concept, someone told me that IBM's AIX has been rated B1; can anybody inform me, whether this is true?)

Despite of such insight (even of their employees), several manufacturers try hard to sell UNIX systems to banks, medical institutions and state agencies, in conscious contradiction to Grampp/Morris insight. While specially protected `production systems' are neither available nor developped, the installation, first isolated but later integrated into complex systems, of such inherently insecure systems will inevitably produce a `big bang' in some not to distant future: the criminal potential is deeply embedded in the systems, more than in their abuse.

While the Virus-Worm did evidently produce only limited damage (esp.

`eating' time and intelligence during a 16-hour nightshift, and further distracting activities in follow-up discussions, but at the same time teaching some valuable lessons), the consequence of the UNIX euphoria may damage enterprises and economies. To me as an educated physicist, parallels show up to the discussions of the risks overseen by the community of nuclear physicist. In such a sense, I slightly revise Peter Neumann's analogy to the Three-Mile-Island and Chernobyl accidents: the advent of the Virus-Worm may be comparable to a mini Three-Mile Island accident (with large threat though limited damage), but the `Chernobyl of Computing' is being programmed in economic applications if ill-advised customers follow the computer industry into insecure UNIX-land.

Klaus Brunnstein University of Hamburg FRG

Unauthorized Access

"Dennis G. Rears (FSAC)" <drears@ARDEC.ARPA>
Sat, 12 Nov 88 13:37:18 EST

Dave Bozak writes:

> Clearly the design and release of a worm is a violation of
>section 156.10. The worm was released was intended to gain access to
>machines without authorization and was designed to gain access to
>material (host lists) for propagation of the worm.
> Now maybe I am missing something here, not being a lawyer...so
>would learned colleagues please clarify the legal issues involved
>in this particular case?

The key is "unauthorized access". The sendmail process from the target machine allowed him to access it. He did not access that process without authorization; he just gave it something it didn't want. Sendmail accepted it. Because of that, he did not brake that law.
The main problem with making worms/viruses illegal is drafting the laws. What is authorized access? If a friend of mine on Computer "A" gives me his password; does that in itself give me authorized access? Since I am on the milnet I can fing, ftp anonymously, send mail to lots of computers. All of these actions I have implied authorization. When dealing with networks the laws have to prohibit actions once access is made not prohibit access.

Dennis G. Rears: Computer Scientist, 1LT USAR & Civil Servant
AT&T: 201-724-6639 SMCAR-FSS-E, Bldg 94, Picatinny Ars, NJ 07806

---

re: NY Computer Laws and the Internet Worm

Forrest Colliver <fwc@mitre.arpa>
Sat, 12 Nov 88 16:55:11 EST

With respect to the apparently "obvious" breaking of laws in the Internet worm case, bear in mind that the FBI only has jurisdiction in cases which involve federal crimes, or in cases where a suspect crosses state lines in conjunction

with unlawful activities which would otherwise fall into state or local jurisdiction. Thus, breaking of NY state laws would not automatically allow the FBI to begin an investigation. It does seem that the progress of the worm across state boundaries would allow the FBI to assume federal jurisdiction, but I suspect that without precedents to fall back on, the legal profession is proceeding with caution!

F.C., The MITRE Corp., Washington, D.C.

Re: NSA attempts to restrict virus information

smb@research.att.com <Steven Bellovin>
Sat, 12 Nov 88 22:49:54 EST

The situation is rather worse than the Times and AP have reported. The NSA is exerting a great deal of pressure to have disassembler output from the virus (to say nothing of C source) available to as few people as possible. When they learn of a copy in a repository (say, available for anonymous FTP), they ask their contact -- perhaps an administrator, perhaps a name they happen to know at that school to remove it. If that person hesitates, or expresses a wish to contact the person who made it available, they immediately contact the president of the university, who calls the dean, who calls, etc. As best I can tell, they have no legal authority to order the removal. But they are not hesitating to bring as much pressure to bear as they can, to try to scare folks into complying.

--Steve Bellovin

Risks of unchecked input in C programs

<wcs@alice.att.com>
Sun, 13 Nov 88 22:31:43 EST

In RISKS 7.74 Geoff Collyer wrote about the finger-daemon hole caused by gets's lack of checking on the size of the input, and called for gets's eradication ("A bug waiting to happen"). While the ancestry of gets is certainly dubious, scanf() suffers from the same problem as commonly used (do *you* always use %50s instead of %s? "man scanf" doesn't).

I've always been dissatisfied with the printf/scanf family - field widths are hard-coded in the format strings, with no way to parameterize them except building format strings on the fly, and there's no nice way to read/print arrays except character strings. It would be nice to say

```
   int i, data[NITEMS]; char *string;
   string = emalloc(whatever);
   scanf("%nd %ns", NITEMS, data, whatever-1, string);
```

and know it would read the correct amount of data into each array,
and to write printf("%n10f\n", 4, data);
instead of printf("%10f%10f%10f%10f\n", data[0], data[1].....);

Bill Stewart ho95c.att.com!wcs AT&T Bell Labs, Holmdel NJ

Re: Risks of unchecked input in C programs (RISKS-7.74)

bobf@lotus.UUCP <Bob Frankston>
Mon Nov 14 10:05:25 1988

The "little care" necessary to use the string functions safely amounts to reimplementing them which renders them pointless but they are very dangerous in that the "not so careful" are so numerous.

Worms & Ethics

Don Wegeng <Wegeng.Henr@Xerox.COM>
14 Nov 88 16:52:23 EST (Monday)

In reference to the recent Internet Worm incident, I was going through my library last night and found that CACM vol. 25, no. 3 (March 1982) contains two relevant articles. The first is the well known Worm paper by Shoch & Hupp, immediately followed by "A Self-Assessment Procedure Dealing with Ethics in Computing," edited by Eric A. Weiss. In light of recent history this is an interesting coincidence.

Perhaps we should teach Computer Science students to read the entire journal issue when they're reading papers on a particular topic. :-(
/Don

One count, or multiple counts?

<Richard_Wiggins@um.cc.umich.edu>
Mon, 14 Nov 88 09:51:32 EST

The Federal law that's been mentioned as the likely tool for prosecution of Morris Jr makes the first transgression a misdemeanor and subsequent ones a felony.

The question is, did Morris invade hundreds of computers, or did he invade one network?

As they say, "the network is the system." And it appears that he fired only one salvo -- albeit with 3 warheads.

-- Rich Wiggins, Systems Programmer, Michigan State University

The RISKS of jargon

Dave Horsfall <dave@stcns3.stc.oz.au>
Fri, 11 Nov 88 14:17:00 est

One of the RISKS in the use of computers is that it engenders a jargon that is

at odds with community acceptance e.g. "ram", "mouse" etc.

Here is an example of such a RISK that is the other way around, taken (without permission) from the "Backbytes" page in "Computing Australia", Nov 7, 1988:

``Well, it sounded like an opening.

> Some chipocentric people have difficulty accepting that computers aren't the centre of the universe (Whoops! Is IBM reading this?). Or perhaps it's just that the jargon of the public service is enough to throw even computer aficionados (masters of their own gobbledegook). Whatever, DDP's state-of-the-art Canberra rep thought he had the makings of a sale recently.
>
> Spotting a Dept. of Arts, Sport, Environment, Tourism and Territories [yes, Australian bureaucracies are like that!] advertisement inviting tenders for the "supply and installation of a restricted keying system", Richard Presser's white-haired boy thought: "We've got just the thing, our Rode/PC!"
>
> This esoteric device delivers dedicated data entry system performance, which is to say, it's a keying system. At least in computing argot. That very day he wrote off requesting more details and, of course, tender forms. To his great astonishment, it turned out what the department actually wanted was 108 locks for lockers and and other equipment at the Fraser (ACT) Primary School.

-- Dave

University of Surrey Hacker

Brian Randell <B.Randell@newcastle.ac.uk>
Thu, 10 Nov 88 19:14:00 GMT

There has been a lot of recent publicity in the U.K. about the arrest of a hacker at the University of Surrey. There were stories about his investigation by Scotland Yard's Serious Crimes Squad and by the U.S. Secret Service, and much dicussion about the inadequacy of the law relating to network hacking - as far as I know he has only been charged with offences relating his unathorised (physical) entry to the University buildings.

An article in today's Guardian newspaper that is based on an interview with the individual, one Edward Austin Singh, reveals that his techniques were simply based on a program which tricked users into unsuspectingly revealing their passwords. "I wrote a program that utilised a flaw that allowed me to call into the dial-up node. You always do it by phoning, never by the network. The dial-up node has to have an address as well, so we were calling the address itself. I called the dial-up node via the network and did it repeatedly until it connected. That happened every 30 seconds. It allowed me to connect the dial-up node at the same time as a legitimate user at random. I would then emulate the system."

He used to run this program at night, and specialised in breaking into Prime computer systems: "I picked up about 40 passwords and IDs an hour. We were picking up military stuff like that, as well as commercial and academic", he claims. This enabled him to get information from more than 250 systems world-wide, and (he claims) in concert with an underground hackers network, to "access virtually every single computer system which was networked in the US - thousands and thousands of them, many of them US Arms manufacturers".

The article states that "Prime Computers have so far declined to comment on his approach to them or his alleged penetration of their computer systems, until the American Secret Service completes its enquiries."

Brian Randell

Re: UK vehicle-identification systems

<denbeste@OAKLAND.BBN.COM>
Mon, 14 Nov 88 09:16:05 -0500

I find Chaz's description of the new system in Britain for toll-roads very interesting, to say the least. I have some interesting questions:

1. As I understood it, what we have is a radio handshake between each car and fixed tranceivers at the entrance and exit from the toll-road, presumably connected to a computer billing system which mails you a bill each month. What if you move and don't tell the computer your new address?

2. The idea is that with this mechanism it won't be necessary for the car to stop or slow down, as we must do here on the Masspike with traditional toll booths. More interesting is that it will presumably work in heavy traffic at high speeds. Not only won't it be necessary for the car to slow down, it can't do so without causing an accident. So if for any reason the handshake fails, the system has no recourse. Which leads to the interesting speculations:

3. The handshake happens at a certain radio frequency. What happens if the car happens to carry a low-power RF noise generater at just that frequency?

4. What happens if someone figures out how to get into their car's tranceiver and change the signature? It doesn't even have to be a valid one because there isn't any way for the highway to stop the car or log what it is.

5. What happens to cars which have crossed the Channel from France? Here in Massachusetts we have people who register their cars in New Hampshire to avoid the property tax (illegal, by the way); will Brits be registering their cars in Brittany to avoid the highway tolls?

6. Everything screws up. I can see the following scenario: John drives the A13 (or some other typical highway designation - I made this one up based on, sigh, Monty Python) to work every day. On Friday he gets on it (handshake succeeds) and drives home and gets off it (handshake fails for some odd reason - a nearby lightning strike just during the handshake?); Monday morning he gets back on it to go to work (another lightning strike louses up the handshake - isn't the

weather *terrible* this time of year?) and gets off it near his job (handshake normal).

What does the computer see? It sees John getting on Friday evening and not getting off until Monday morning. John sure must have driven a lot of miles that weekend - let's bill him big.

7. Just what WILL the computer do with a partial transaction - get on but don't get off, or vice versa? I can think of many ways this could happen.

8. Since there will be some cars on the highway without tranceivers (French etc.) then the system can't scream when it sees one. What is to keep someone from driving an ice-pick through their tranceiver with a hammer, or much more simply, pulling its fuse or clipping its power lead? Will the British meter maids start carrying little tranceiver-testers around checking every parked car to see if its tranceiver will handshake? The mind boggles. (I think that pulling the fuse is the best answer - that way you can plug it in again just before the yearly equipment check.)

Frankly, it sounds like the greatest target for hackers since the ARPAnet!

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

UK vehicle-identification systems

<fad@Think.COM>
Mon, 14 Nov 88 14:52:19 EST

In his 10 Nov 88 RISKS contribution, Douglas Jones discusses optical and microwave barcode scanner devices for collecting tolls from cars. He states:

> The risk of such sensors as police devices depends to a great extent on how easy it is to instrument locations in the roadway without the driver being aware of it.

Why not make use of such a system voluntary? If I had a choice between lining up to drop coins in a gate vs. driving through a barcode-reading gate, I'd choose the latter, assuming it meant I wouldn't have to come to a stop. But anyone who prefers anonymity could always use the regular toll gate (where presumably no one is writing down license plate numbers) and not install the barcode on their vehicle. The principle seems to me to be that if you are potentially diminishing someone's privacy, they should have a choice about it, and the costs and benefits should be made clear.

--Franklin Davis Thinking Machines Corporation fad@think.com

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 78

Tuesday 15 November 1988

Contents

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

Computers in Elections

Peter Neumann <neumann@csl.sri.com>
Tue, 15 Nov 1988 11:10:34 PST

Readers of the references given in RISKS-7.52 to 54, and 7.70 to 71 (the New Yorker article by Ronnie Dugger, and reports by Roy Saltman; Lance Hoffman; Bob Wilcox and Erik Nilsson; and Howard Strauss and Jon Edwards) know that at least five past elections have been legally challenged on grounds of fraud. In all of these cases, the same company (BRC, formerly CES) provided the computing services. The lawsuit in Indiana is still in process.

The latest item on the integrity of computers in elections relates to this year's Senate race in Florida. The New York Times (Saturday, 12 Nov 88, page 9) had an article by Andrew Rosenthal on suspicions of fraud arising from the results. At the end of the Election Day ballot counting, the Democrat Buddy Mackay was ahead. After the absentee ballots were counted, the Republican Connie Mack was declared the winner by 30,000 votes out of 4 million. However, in four counties for which BRC provided the computing services, the number of votes counted for Senator was 200,000 votes less than the votes for President (i.e., 20% less), while in other counties and in previous elections the two vote totals have generally been within 1% of each other. Remembering that these computer systems reportedly permit operators to turn off the audit trails and to change arbitrary memory locations on the fly, it seems natural to wonder whether anything fishy went on. I hope that our Florida readers will keep us informed of any further developments.

Risks in econometric models

Ross Miller <rmmiller@bu-cs.BU.EDU>
Mon, 14 Nov 88 16:36:19 EST

On the front page of the Sunday N.Y. Times, Peter Neumann raises a computer security related risk that I have not seen discussed before. At the end of his piece on describing the potential for viruses spreading, he states, "Do we know the econometric models of the country are correct, for example?" As a once and sometimes econometrician (who does microeconomic rather than macroeconomic work), I found this question to be one that is worth examining.

The recent defeat of Michael Dukakis was probably caused in part by the well-publicized fiscal problems of Massachusetts. Did George Bush introduce a computer virus into the state's computers? Probably not. What happened was the effective federal tax rate for capital gains went up, causing investors to rush to take capital gains before the higher rates went into effect, temporarily inflating capital gains tax revenues at both federal and state levels. Because Massachusetts, as well as many other states, considered the increased tax collections as a normal part of revenue growth, they continued to project these gains into the future, when the higher tax rates would prevail. These projections were wrong, and we know what happened.

This risk, however, has nothing to do with viruses, it has to do with the environment in which econometric models are created and used. It should be noted that the econometric modeling industry has been shrinking for several years--many banks have eliminated their in-house forecasting group and subscriptions to outside forecasters are down. The federal government has slashed the funds available for data collection and forecasting activities.

The real risk from traditional computer-based econometric forecasting comes from the lack of new money and talent flowing into the field that keeps the industry from advancing technologically. (If you don't believe me, call a venture capitalist and tell him you'd like to start an econometric forecasting firm.) Conceptual bugs, such as described above, and programming errors are problems that are likely to swamp viruses as a source of error.

Should we worry about all this. No. First, to the extent the such models are used, humans are an important part of the loop. "Fudge factors" are built into every model and unreasonable projections are not used--the model is rerun with new fudge factors. No doubt, just the way programming and conceptual bugs have been "fudged over," a virus would be, too. Second, for most business applications there are much better sources of economic forecasts than large econometric models, and they are essentially free. For example, I can safely state that a reasonable projection of crude oil prices is that they will remain stable over the next year, decreasing a bit over the winter and going back up in summer. Not only that, you can expect long-term interest rates to rise by about 0.5% over the next two years. Did I use a Ouija board or consult my local oracle? No, I just looked up the futures prices in the Wall Street Journal. These are market-generated predictions that are based on the aggregate information contained by the marketplace. True, they do not have

pinpoint accuracy, but they tend to perform quite well on average. As many companies and banks have concluded, who needs big, expensive econometric models? Maybe, just maybe, the marketplace is capable of taking care of some risks, which in this case has nothing to do with viruses, by itself.

Ross Miller Phone: (617) 868-1135
Boston University Internet: rmmiller@bu-cs.bu.edu

[The Times piece consisted of sentences randomly culled from a discursive discussion. The econometric sentence was totally out of context -- relating to integrity and correctness problems, not just worm/viruses, but I'm glad you picked up on it! Thanks. PGN]

Report on SAFECOMP '88 [long]

Tim Shimeall x2509 <shimeall@nps-cs.arpa>
Mon, 14 Nov 88 09:50:52 PST

Report on the IFAC Symposium on
Safety of Computer Control Systems
(SAFECOMP '88)
Safety Related Computers in an Expanding Market
November 9-11, 1988 -- Fulda, FRG (West Germany)

This message is a set of personal observations on the Symposium on Safety of Computer Control Systems, originated and run by the members of EWICS TC-7 with support from IFAC and IFIPS. Prior to this meeting, SAFECOMP was held every three years. This meeting was held two years after its predecessor (SAFECOMP '86 in Sarlat, France) and henceforth is planned to be an annual event (SAFECOMP '89 will be held in Vienna, Austria on September 5-7, 1989).

EWICS TC-7 (Abstracted from a talk by J. M. A. Rata):

The European Workshop on Industrial Computer Systems is a group originally started as "Perdue Europe", a series of workshops held in Europe by Purdue University, it is now sponsored by the European Economic Community. Almost all European nations have representatives in EWICS, with the exceptions being Spain, Portugal and Greece. The majority of members come from France, the United Kingdom and West Germany. TC-7 is the Technical Committee on Reliability, Safety and Security. It's an active group, with a series of technical reports and "Pre-standard" guidelines on computer safety and reliability published at frequent intervals. The current Chair of TC-7 is J. M. A. Rata.

The Workshop:

Over the two and a half days of the symposium, a total of 26 presentations were made. I'm not going to summarize all of the talks, but will give a description of those I found most interesting. The Symposium proceedings are available from Pergammon Press (Edited by W. D. Ehrenberger, ISBN 0-08-036389), but there were 6 talks given at the symposium that were not part of the proceedings - 4 of the papers were distributed on site, 1 was a report of work in progress, and

the last was Dr. Rata's description of TC-7. NOTE: the following are summaries of my notes on the presentations I personally found most interesting. I profoundly regret any inaccuracies, and no criticism should be implied on the papers omitted from this report. [My personal comments are in square brackets - TJS]

Dahll, G., Mainka, U. and J. Maertz*, "Tools for the Standardised Software Safety Assessment (The SOSAT Project)"

This was a description of an environment to aid the licensor of safety-related code. It starts with the final object code of the application to be assessed. This is disassembled and instrumented for comparison with the specification. There are also capabilities for analyzing the disassembled code with commercial tools (e.g., SPADE -- See O'Neill's talk below). SOSAT itself supports 4 types of analysis: Static Analysis, including structure, path and data flow analysis; White-box test data generation; Symbolic Execution; and Real-time timing analysis. The latter was the subject of a presentation by G. Rabe at SAFECOMP '88. It's basically a sophisticated profiler that interfaces directly to the target hardware. [SOSAT clearly has much development ahead, but there seems to be a good start in considering the sort of tools that the licensing examiner may find useful in evaluating safety-related software.]

Bergerand, J.L. and E. Pilaud, "SAGA - A Software Development Environment for Dependability Automatic Controls"

The French cousin of SOSAT is SAGA. This environment is focused more on the development of the code than the licensing. It is basically intended to improve the designs (by supporting design-level analyses) and to support reuse of software modules (with the theory that the more a module is re-used, the better it gets). SAGA has been used to support the development of nuclear power plant control code. It doesn't seem to improve productivity, but the quality of the resultant code seems to be improved.

Fedra, K., "Information and Decision Support Systems for Risk Analysis"

This was a report on a tool to support qualitative risk assessment and disaster planning. It provides a graphic interface to simulate disastrous events and link to databases on related risks, along with geology, geography, weather and population demographics of the region in question. It's geared for non-expert users to support industrial safety decisions. A trial system has been used in the People's Republic of China. The system also has an expert system to support hazard management techniques and support for safety analysis tools like fault-tree analysis. [This was without doubt the prettiest presentation of the symposium, with impressive color graphics showing simulations of Chernobyl, ground-water contamination and population evacuation. However, there were a lot of questions at the symposium about the fidelity of the underlying models used. The basic defense by Dr. Fedra was that the tool does better than the current techniques, supporting safely smaller safety margins. I'm not entirely sure I believe that, given the oft-cite propensity of non-expert users to trust computers too much.]

Taylor, J.R. "Reducing the Risks from Systems Documentation Errors"

The motivation for this work was a case where inaccurate documentation for a circuit board that was part of the firing control system resulted in a

faulty installation that caused a gun turret on a Danish naval vessel to over-revolve and fire at its captain. A subsequent study found that errors in documentation of safety-related subsystems are quite frequent. To reduce these errors, Taylor created the ANNADOC system. The documents are translated by the users into a simplified technical English, which is in turn translated by the system into a set of finite state machines. The FSMs are used to simulate the system so that the documented behavior may be compared with the specified or actual behavior.
[This talk was interesting because of a rarely-considered aspect of safety, namely the affect of the documentation. A member of the audience cited an additional example, a case where incorrect wiring diagrams (known to be incorrect by the management involved and stamped "DO NOT USE", but not corrected) were used in the maintenance of a nuclear reactor. The erroneous wiring caused a reactor trip.]

Panel Discussion: "Is probabilistic thinking reasonable in software safety applications?"

The Proponents of probabilistic thinking cited studies that humans are not deterministic in their behavior, and the desire to be able to use models similar to those used in hardware. The Opponents countered by saying that we really don't have much basis for supporting probabilistic software reliability statements -- if a failure is found during software safety assessment, any reasonable licensing authority will require modification of the software to prevent that failure. The favored approach for the opponents seemed to by careful development and rigorous analysis of the software. A poll of the audience after the discussion showed that a large majority didn't feel that probabilistic thinking was reasonable for software.

Bloomfield, R.E. and P.K.D. Froome, "The Assessment and Licensing of Safety Related Software"

[This is a presentation of an extensive tech report "Licensing Issues Associated with the Use of Computers in the Nuclear Industry", R.E. Bloomfield and W.D. Ehrenberger, Tech Report EUR11147en, Commission of the European Communities, Nuclear Science and Technology, 1988. ISBN 92-825-8005-9. Lots of interesting summaries of the use of computers in various nations for nuclear and safety-related applications. It has a stated purchase price of $24.50 from the Office for Official Publications of the European Communities, L-2985 Luxembourg]

Certification is a formal agreement of the fitness of a system to a specific purpose. There is some transfer of responsibility involved in the certification process, morally if not legally. Certification is normally a large process, with much delegation and summarization. There may be pressures on the certification team to avoid articulating concerns (political and social pressure), to automatically accept subsystems that were generated in response to the certification teams comments, and to ignore a series of small problems that collectively destroy the certifiers confidence in the system. With respect to software, there are several persistent questions:

+ What is the acceptance of risk among the populace and how do the certifiers acknowledge that?
+ How does risk analysis reflect value systems?
+ What are the technological limits?
+ What role should numbers play in certification? If the probabilities are

dominated by common-mode or human-error effects, how should they be evaluated?
+ Should individuals and institutions need to be certified, as well as systems?

Recent work (especially the UK Defense standard that will be published next year) focuses on formal analysis approaches: Z, VDM, HOL, CSS, CSP and use of temporal logics.
[Much here that will be familiar to regular RISKS readers, but useful to see someone from the licensing side articulating these concerns. One member in the audience raised the issue of how one can recognize, or measure, good software engineering practice.]

O'Neill, I.M., Summers, P.G., Clutterbuck, D.L., and P.F. Farrow
"The Formal Verification of Safety-Critical Assembly Code"

A report of a project at Rolls-Royce to certify jet aircraft control code using SPADE. The assembly code was mechanically translated into FDL for analysis, with annotation of proof obligations automatically inserted during the translation. A flow analysis of the FDL code raised queries that were resolved by the implementation team before the proof was conducted. Pre and Post-conditions were derived from module "fact sheets" and manually inserted into the FDL code. The generation of further annotations for the proof was done automatically, but the proof itself involved substantial human interaction. Approximately 100 modules were proven. Total correctness was not proven for all modules, but only about 12 involved loops at all, and the certification team assured themselves that the loops had a fixed limit on the iterations. Each module was verified individually, with no consideration of the inter-modular data flow.

Concluding Session (W. Ehrenberger):
A poll of the attendees of the symposium shows concern for the following problems:
+ Specification of Systems and tools to support this
+ Limits of understanding of the role of software in Safety
+ Man/Machine interface problems
+ Risk reducing tools (How do we qualify the results)
+ Diverging Technology (General approaches seem largely flawed)
+ Reluctance of Industry to use new techniques
+ Robust metrics and measurement (and how it relates to political acceptance of risk)
+ Identification of Critical system components and critical failures

[Ehrenberger noted that many of these concerns were unchanged since the first SAFECOMP in 1979 -- a recognition that we have a long way to go. It seemed to me that this was a fair summation of the entire symposium. Some approaches look promising, but we have a long way to go to really address the problems. The papers were strong in recognizing the issues, but there was a large gap between the acknowledged problems and the proposed solutions.]

*Note: Umlauts are interpreted by using the "following e" convention. Thus, a-umlaut is written as ae, etc.

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 79

Wednesday 16 November 1988

Contents

- Vote Count Error
  - Kenneth R Jongsma
- Computer Ethics Class
  - Leslie Chalmers
- Teaching "Ethics"
  - Eric Roskos
- Re: NSA attempts to restrict virus information
  - Theodore Ts
- The FBI Wants You (if you were virus-ized)
  - Tom Zmudzinski via Dave Curry
- Access and authorization
  - Joe Morris
- Laws of computer evidence
  - Barry C. Nelson
- Call for comments on uniformity legislation for software
  - Conleth S. O'Connell via Alan Kaminsky
- Info on RISKS (comp.risks)

Vote Count Error

<portal!cup.portal.com!Kenneth_R_Jongsma@unix.SRI.COM>
Tue, 15-Nov-88 15:07:56 PST

The following article appeared in the local paper. I'm sure it will be the first of many to appear after the recent elections. I will try to refrain from commenting. There are so many obvious issues raised here!

Tally Error Gives Logan Clear Win

(Exerpted Without Permission)

Attorney Benjamin Logan won the write-in race for Grand Rapids District Judge by 461 votes - not just 20, the Grand Rapids city clerk's office announced today after finding the error.

The computer processing system designed to handle the write-in race did not pick up the vote tallies from five precincts on the city's southeast side - Logan's strongest area.

Those votes make it virtually certain that the Board of Canvassers' rulings on name variations will not change the outcome.

City Clerk Sandra Wright said no other races were affected by the computer problem. A seperate computer program counted ballot cards for the other races. The system used for the write-in election was a Lotus 1-2-3 computer program developed by local staff, she said.

Tom McQuillan, director of management information systems for Grand Rapids, said

the error apparently stemmed from a problem with the computer program, which ordered the computer to tally 3rd Ward votes starting with the sixth precinct, rather than the first. "It's not what we call a computer error," he said. "It's a human error."

Wright said she discovered the problem Saturday night while adding up the figures from the race manually. "I found the 3rd Ward was inconsistent," she said. "I was further able to isolate that we were not picking up tallies in Precincts 1,2,3,4 and 5."

(Explanation of Judges duties, salary, and reason for write-in contest deleted)

McQuillan said the error may have been inserted in the program after the city staff ran it through a test run. The program was (then) modified so subtotals could be released while the votes were being tallied and the original computer formulas may not have been rechecked. ("But Boss, I just need to make this minor change. It can't possibly hurt anything!)

Voters in the five precincts that had not been counted cast 604 votes for Logan and 163 votes for Christensen. (Enough to change what was a virtual dead heat that would have had to have been decided by the Board deciding what a voter's "intent" was when they misspelled a name on the ballot, into a solid victory for Logan.)

Computer Ethics Class

<Chalmers@DOCKMASTER.ARPA>
Tue, 15 Nov 88 15:48 EST

Regarding Bob Barger's entry, "Comments sought on proposed computer ethics course" (RISKS 7.75), I was frankly shocked at the statement "There will be no class meetings, except for the first and last sessions. Students will instead utilize electronic bulletin boards on the university's mainframe computer network to research and discuss issues."

It has been a long time since my college days and I may be hopelessly out of date on these matters, but why on earth would one conduct any class, and

particularly one on ethics, without any class time?

One of the problems with the computer 'hackers' of today is their isolation from others in society who might disagree with their point of view. Allowing students to 'participate' in a course via a terminal only encourages this isolation. While a majority of students might agree on what we would consider ethical behavior, some will not. It is important that such students be subjected to the direct challenge of their classmates. Group interaction is critical for this purpose.

I would further suggest that Barger make a point of including in his class, lectures by people who have suffered negative consequences from the activities of individuals who do not believe that other computer users have any rights other than those they grant themselves by building secure systems. Just as a judge recently ordered a notorious slumlord to spend time in his own buildings, people who have a belief system that condones computer hacking should be forced to face the victims of such activities.

In the case of computer ethics, there is very little that even those of us in computer security can say is *unambiguously* "right" or "wrong". There are activities which we could agree are inconvenient or destructive for other users of computer systems such as denial of service or erasure of files. We could even come up with some empirical evidence of the consequences of these activities to prove that they are inconvenient or damaging (deadlines missed because report was erased, man-hours, excuse me, person-hours spent locating unauthorized code and purging system, etc.) But I have read quotes from 'hackers' and even some participants in this forum suggesting their firm belief that anyone who does not protect himself from hacking *deserves* what he gets. It would seem to me that one of the objectives of an ethics class should be to modify that point of view.

There are things which may be unambiguously "illegal" (though precious few), but this is not the same thing at all. As one who came of age in the '60s, I can attest to the irrelevance of the legal system to people who believe in their heart of hearts that the laws are wrong. If we '60s students had blindly accepted the notion that whatever is "illegal" is ipso facto "wrong", life would be very different today. Clearly, ethics has only a casual relationship to legality. The purpose of an ethics course should be to convince students of the importance of a code of behavior and a social context is essential for getting that message across.

Leslie

The standard disclaimers apply.

Teaching "Ethics"

Eric Roskos <roskos@ida.org>
Wed, 16 Nov 88 16:01:14 EST

> Perhaps if everyone were exposed to ethics courses, beginning in the
> early grades and continuing through computer ethics courses and business
> ethics courses, etc, then it would be clear `in the entire community

> what is and what isn't ethical behavior.'

Unfortunately, this is much more complex than it first appears; I wonder how many people who recommend "ethics courses" have ever taken an ethics course.

Henry Thoreau once observed that whenever he tried to argue rationally with someone, the person would agree with him repeatedly up until the time his final conclusion became evident, at which point the person would vehemently refuse to accept the conclusion, eventhough he had accepted all the premises leading to it.

This is the case with ethics. People all agree that everyone should behave "ethically," yet they refuse to agree on what precisely is ethical behavior. In an Ethics course, the most you can do is discuss ethical paradigms, which include systems of ethics in which it is entirely acceptable to engage in any activity that benefits you ("situation ethics" are an example of this). "Ethics" differs from "a specific set of ethical principles"; after all, "there is honor among thieves".

This is not to say that I advocate irresponsible behavior; and, in fact, I attended a college which had a working "honor system" and a working "code of responsibility," and think they were successful in teaching ethical behavior to the students. I just don't think that calling for "ethics classes" is going to accomplish the desired end. And I don't think there is enough agreement on what should be taught to do so.

Note, however, that the ACM has a code of ethics. Perhaps we should focus on more effectively conveying it, as I fairly often see people violate it in the RISKS digest.

Eric Roskos, IDA (roskos@CS.IDA.ORG or Roskos@DOCKMASTER.ARPA)

Re: NSA attempts to restrict virus information

Theodore Ts'o <tytso@ATHENA.MIT.EDU>
Tue, 15 Nov 88 02:45:16 EST

Steve Bellovin noted that the NSA was "exerting a greal deal of pressure th have dissassembler output from the virus (to say nothing of C source) available to as few people as possible...." He then went on to say that they were leaning on contacts, such as the president of the university, etc. Before people raise their hackles and get up to call the ACLU, I'd like to make a few points:

First of all, the only incident that I know of where this happened was at Purdue, where the NCSC (the public arm of the NSA) leaned on the president to remove a copy of the disassembler output from an anonymous ftp directory. They went into hysterics when they thought that a copy of C source code of the virus had been posted to phage, a mailing list which has several hundreds of people on it, but they didn't (couldn't) do anything about it. (In actual fact, it was only a partial decompilation of the virus --- about 15-20%.) In fairness, they were

probably over-reacting after the initial shock/aftermath of the virus.

If the NCSC has tried surpressing it elsewhere, I'd like to know about it --- but it seems that Steve was generalizing from only one data point. Or perhaps he got the information from the Markoff column in the NYT recently. I really think that column was badly written or perhaps badly edited --- someone apparently did not understand all of the issues involved.

Secondly, trying to limit the source code to the decompiled virus is a good thing. If it were publicly distributed, there's a chance that some person will find another security hole and just drop it into the virus ``body'' that the source code would provide. In addition, they might add some malicious code so that after 12 hours or so, would try to destroy as many files as possible. Someone might just disable the fingerd and sendmail hack; the virus might still be able to propagate far just cracking stupid password choices.

There are also legal issues: if someone releases the code, and someone uses the code to make a really damaging virus, is the person who released the code liable? Does someone want to take that risk and find out the hard way?

In addition, one of my colleagues is currently writing a paper that will describe, in detail, all of the algorithms used by the virus. The paper will be published for general reading, and should be infinitely more useful than the actual source code. That is, there is no legitimate purpose that would require the source code over the algorithms. The only purpose for obtaining the source code itself would be to build another virus.

If a determined cracker wanted make another virus, yes, he could use the algorithms. But as the paper will demonstrate, those algorithms weren't the best anyway, and very little will stop someone that determined. It appears that it took RTM at least a few weeks to write it from scratch --- and he knew Unix fairly well.

Not releasing the source code is intended to stop the ``Freshman Twit'' who knows how to type `system("rm -rf /");` and `cc`. Unforunately, many universities (including MIT) are connecting to the Internet, and we get a constant stream of new-comers to the Internet community --- most of them have only PC programming as their background, and no concept as to the ethics involved. Who knows what they might do?

According to a colleague who was at the ``Virus Conference'' at Washington called by the NCSC, they had agreed with our decision (which we had made before talking to them) of only distributing the algorithms and not the source code to the virus.

- Ted

The FBI Wants You (to call if you were virus-ized)

<davy@riacs.edu>
Tue, 15 Nov 88 08:12:57 -0800

The enclosed message was sent to the TCP-IP list. As per its request to give it maximum distribution, I am forwarding it to RISKS. What with all the speculation on how the FBI is going to (try to) prosecute, it is useful for its information content as well.

I would strongly urge everyone who wasted their time cleaning up after this mess to respond. Regardless of whether you feel Morris (or whoever) is a hero or a scumbag, it is important to note the last line of the message - if we want the FBI to help us when something truly serious happens (and you know it will...), then we had better show them we're willing to help them now. Otherwise, they may just ignore us next time since we were unwilling to cooperate.

--Dave Curry

From: TomZ@DDN1.ARPA
Subject: FBI Contact re: November Internet Virus
Date: 14 Nov 88 05:03:00 GMT

Were YOU hit by the November Internet Virus?

The FBI wants to hear from you!

The Federal Bureau of Investigation is attempting to gather critical information necessary to pursue this case under the Computer Fraud and Abuse Act of 1986. (This is the statute that makes it a federal crime to penetrate a computer owned by or run on the behalf of the Government.)

The FBI Case Agent has asked the Defense Data Network Project Management Office to collect the names of organizations and Points of Contact (names and phone numbers) that were hit by the Virus. The Defense Communications Agency has established an E-Mail address for this collection at:

INFO-VACC [at] BEAST.DDN.MIL

Points of Contact should expect to be contacted by their local FBI agents for dispositions due to the wide geographical area involved.

I * M * P * O * R * T * A * N * T

The FBI needs this information to pursue the case.

If we expect their aid in the future, we need to help them now.

PLEASE GIVE THIS MESSAGE MAXIMUM DISTRIBUTION; NOT EVERYONE IS ON "TCP-IP"!

/s/ Tom Zmudzinski, DDN Security Officer (703) 285-5206

access and authorization

Joe Morris (jcmorris@mitre.arpa) <jcmorris@mitre.arpa>
Tue, 15 Nov 88 17:34:04 EST

In Risks 7:77 Debbus Rears comments:

> The main problem with making worms/viruses illegal is drafting the laws.
> What is authorized access? If a friend of mine on Computer "A" gives me his
> password; does that in itself give me authorized access? Since I am on the
> milnet I can fing, ftp anonymously, send mail to lots of computers. All of
> these actions I have implied authorization.

There seems to be a problem here in distinguishing between authority to access a facility and the authority to perform some action once the access has been successful. For example, if I am allowed to go into the stacks of a library, that does not imply that I have authorization to tear out pages from books I find there.

Most computer facilities prohibit the use of an account by anyone other than the individual to whom it was assigned. Your friend probably had no authority to give you the password, and you have no authority to use it. The fact that you can masquerade as your friend by supplying his userid and password in no way implies legality of the action.

The TAC access cards from DDN have a section which reads:

> Authorized use of the DDN is limited to the conduct of or support of government business.

So if you start a chain of events which you know will involve DDN facilities (even if you aren't directly connected to it) then your authorization is limited to activities on behalf of Uncle. The fact that you're on MILNET means only that you (supposedly) have authority to be on MILNET. What you do once you're there is a different question.

---

laws of computer evidence

"Barry C. Nelson" <bnelson@ccb.bbn.com>
Tue, 15 Nov 88 20:13:55 EST

How fascinating is this collision of the mathematical with the societal -- where the common law meets the computer (user)! Two recent cases in point...

Does the UK Vehicle Ident system differ much from the already-admissible credit transaction records. "By the records, something you control (car, credit/ATM card) was used at that location, so is there any proof it wasn't used by YOU?"

On another topic, the problem facing the FBI may not be so much one of finding a statute that Morris violated as being able to construct the necessary case based on acceptable (and attributable) EVIDENCE that he actually broke that law.

Rules of Evidence indicate that "any printout or other computer output readable by sight, shown to reflect the data accurately, is an 'original'" for purposes of demonstrating existence of "writings and recordings" as evidence.

This implies that copying a program to another computer creates the source of another "original". If the creation and use of the first original was a crime, was creation and use of subsequent "originals" also a crime? Only some? Which?

If someone could point me to a good text on the topic, I'd appreciate it.

Barry C. Nelson

Call for comments on uniformity legislation for software

<ark%hoder@CS.RIT.EDU>
Tue, 15 Nov 88 09:51:10 EST

[The message below recently appeared in the Usenet comp.software-eng newsgroup. Since I think it will be interesting to RISKS participants I have submitted it verbatim. -Alan Kaminsky, Rochester Institute of Technology]

> [Please respond directly to Conleth O'Connell and ask that the results be made available to RISKS. PGN]

Conleth S. O'Connell at Ohio State University writes:

I have been asked to get opinions (both positive and negative) on the feasibility of drafting "uniformity legislation" for software.

Uniformity legislation affects everyone in the U.S. and its territories equally. While there may be variances in the law of a particular state, the fundamental law will be the same everywhere. For example, uniformity legislation in the U.S. requires that cars meet certain minimum pollution standards, but individual states are free to mandate higher standards.

A government committee is now considering if uniformity legislation for software is necessary, warranted, or desirable. For example, should software suppliers be required to warranty their products? should suppliers be required to inform users of known bugs? should bug-fixes be distributed at cost? who should be responsible for viruses in object code? etc.

If you have an opinion on software uniformity legislation, please express it publicly, and I will forward your thoughts to one of the committee members. If you feel moved to "second" an opinion already expressed, please send me e-mail.

Thank you,
Conleth S. O'Connell Department of Computer and Information Science
cso@cis.ohio-state.edu The Ohio State University
2036 Neil Ave.

Columbus, OH USA 43210-1277

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 80

Friday 18 November 1988

Contents

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

Computer glitch causes Fresno `flood'

Peter Neumann <neumann@csl.sri.com>
Fri, 18 Nov 1988 14:27:22 PST

FRESNO -- The computer that controls the city's water service malfunctioned, or ``crashed'', three separate times Monday within an hour and a half, causing at least 12 mains to rupture and damaging nearly 50 residential plumbing systems.

The $2.3 million computerized telemetering system, which has been in operation for only six months, controls 106 water pumps and wells and 877 miles of piping.

... the malfunction -- which centered in a burglar alarm at one of the pumps -- sent confusing signals to the computer that temporarily shut down the pumps.

An automatic restart device that shifts the system over to manual controls sent water pressure levels of up to 75 pounds per square inch surging through the pipes. Usually the level ranges from 40 to 45 [ppsi].

With the computer inoperable, the manual system took over with each pump operating on its own fixed settings. ... the settings apparently weren't properly set and the resulting heavier flow of water proved too much for some

of the city's older mains to handle.
It also triggered 24 automatic fire alarms ...

[From the San Jose Mercury, 16 November 1988, thanks to Ira Greenberg]

Election Computing

Peter Neumann <neumann@csl.sri.com>
Fri, 18 Nov 1988 16:03:04 PST

A law suit has just been filed in Texas on behalf of the voters of the state challenging the entire election and requesting not a recount but an entirely new election. The grounds are that the State did not follow its own procedures for certifying the election equipment. Perhaps one of our Texas readers can keep us informed of the details.

Re: Vote Count Error

Brint Cooper <abc@BRL.MIL>
Thu, 17 Nov 88 11:53:34 EST

Re: Kenneth Jongsma's contribution on vote count error.

Back in 1958 (!), the Black & Decker Co. was converting their inventory records to an automated (they didn't do "computers" then) system. Among my duties as a summer student trainee was to copy data from those dull, yellow inventory cards to forms from which keypunch would be done.

The chap in charge of the project told us that they would run the manual and the automated systems in parallel for one full year before abandoning the manual system. These folks had a very healthy respect for "the unknown" and sought to minimize their risks.

Have we forgotten what we've learned? In something so important as an election, why are not the votes counted "manually" as well as by the "new system" until all the bugs are worked out of things such as Lotus scripts. It's such a simple idea that we assume it must have occurred to our political leaders and the Boards of Elections when, in fact, it probably has not.

_Brint

Casiers numeriques! (Digital lockers!)

Marc Vilain <MVILAIN@G.BBN.COM>
Thu 17 Nov 88 14:41:49-EST

While in Paris last week, I stopped at the luggage check of the Gare du Nord train station to drop off a suitcase. To my great surprise, the familiar cluncky keyed lockers had been replaced by their gleaming high-tech equivalent.

The French, who so enthusiastically brought us Minitel, now have computerized luggage lockers.

The basic unit is a block of six lockers which are shut by some kind of servo latch. The six lockers share a little keyboard and LED display. It works like this: You put your baggage into a free locker, close the door, and drop FF 15 (= $US 3) into a coin slot. The machine latches your locker door and prints out a little ticket indicating the identification number of your locker and a 5-digit password, apparently generated at random. When you want to retrieve your bags, you key in the password and, voila, the locker door opens up.

The locker system guards fairly well against the most obvious security flaw: a nefarious individual reading the code on the ticket as it is printed out. The ticket is actually printed on a double strip of paper. The writing only appears on the inner strip, and you have to peel away the outer one to read the password.

Throughout my stay in Paris, I wondered how the lockers guarded against a brute force attack on their password. I found out as I was retrieving my bags. Near me a group of clearly puzzled passengers were trying to collect their own belongings, and were typing away on the keyboard of their locker. Suddenly, a siren sounded from the bowels of the locker, alerting the attendant in charge of the luggage check -- the befuddled passengers must have typed one password too many.

Befuddlement, unfortunately, seemed the general response of newcomers to these clever machines. I used these lockers several times during my stay, and I never failed to see perplexed faces staring at the instructions. Given that France seems to have pushed computer literacy in a big way recently, one may view with some degree of pessimism the success of the enterprise. But perhaps I should be more charitable -- I too was confused at first.

Re: Toll Road information collection

David Phillip Oster <oster@dewey.soe.Berkeley.EDU>
17 Nov 88 13:04:08 GMT

Many toll roads in the U.S. give you a ticket at the spot you enter the toll road, and collect the ticket when you leave. The tickets are stamped with their origin, so the distance driven can be computed. So far so good.

Is it fair to also stamp the tickets with the time of issue, so if the distance traveled divided by the time elapsed is greater than the average speed limit the toll taker can hand you a speeding ticket at the same time? An appropriate computer would help the toll taker in this task.

Massachusetts has drastically higher fines the faster you go. The above system can only conclude that your average speed was above the legal limit.

If there is a monitoring system measuring when your car crosses each sensor, every ten miles say, then the system can draw conclusions about your speed on the inter-sensor segments of your trip. Segments at 80 mph can be fined

at a much greater rate than those at 60.

Do people have a right to violate the speed laws? If not, should the state be making investments in speeder catching gear so long as the "take" is more than the capital cost?

A related question: Where can I buy a radar gun, and how much do they typically cost? I want to aim one at speeders to make their radar detectors sound off.

--- David Phillip Oster --When you asked me to live in sin with you
Arpa: oster@dewey.soe.berkeley.edu --I didn't know you meant sloth.
Uucp: {uwvax,decvax}!ucbvax!oster%dewey.soe.berkeley.edu

Risks of non-technologists' reactions to technological failures

<mccall@skvax2.csc.ti.com>
Fri, 18 Nov 88 17:46:03 CST

There seems to be a genuine risk involved with regard to public perceptions of complex and little understood technologies, in that when the inevitable failures occur there is an unthinking overreaction, based, I suppose, upon disappointed expectations of perfection in technology.

In the wake of the inevitable failures involving a technology, those who don't understand the issues are prone to call for sweeping changes to 'correct the problems'. This is similar to outcries against 'electric jets' in the wake of the Airbus crash in France and against NASA after the Challenger incident (although in my opinion, NASA was more than ripe for it).

Those who call for the most drastic measures with regard to issues they know nothing about are often the most adamant in adhering to their belief that the 'elite' are really conspiring to cover things up.

For instance, with regard to the article that follows, when I attempted to correct some of the factual errors I found myself subjected to public abuse. Pointing out errors in the usage of words with regard to 'virus' and 'hacker' earned comments about refusing to write to pander to "the incestuous coterie of computer insiders" and comments about how the perpetrator of this act is really the one to blame and that laws about this sort of thing need to be enforced if we're ever going to stop them rather than simply regarding them as 'pranks' evoked phrases about "the neo-fascists of the computing world" and about how enforcing laws isn't the solution.

When someone who is a reputable journalist is reacting in this way, what solutions are there to risks involved in people misunderstanding the technology and events associated with it?

I wonder how many articles like the following are appearing in various places around the country in the wake of the Arpanet worm? The fact that

it's by someone who describes himself as a "technology writer" and "computerist" and who is involved in reputable journalism only makes the point more strongly.

[Article and the author's online profile follow.]

==
Fred McCall (mccall@skvax1.ti.com)	My boss doesn't agree with anything
Military Computer Systems	I say, so I don't think the company
Defense Systems & Electronics Group	does, either. That must mean I'm
Texas Instruments, Inc.	stuck with any opinions stated here.
==

================================== ARTICLE ==================================

AL FASOLDT

Technology writer (syndicated newspaper columnist) and audio writer (Fanfare Magazine), newspaper editor in Syracuse, NY (the daily Herald-Journal), poet, bicyclist, computerist who loves simple programming; a fan of the Atari ST and no fan at all of MS-DOS computers; 2 grown children.

1 (of 7) AL FASOLDT Nov. 14, 1988 at 20:48 Eastern (4846 characters)

Let's start things off with some thoughts on who is really responsible here.

This is an article I wrote for distribution this coming week.

Publication date: Nov. 20, 1988

By Al Fasoldt

There's an untold story in the furor over the electronic virus that infected 6,000 mainframe computers across the country earlier this month.

Left out of the many accounts of the prank pulled by a Cornell graduate student is something that could be the single most important issue of computer networking in the next decade.

It is put most simply in the form of a question: Who is in charge of our mainframe computer networks?

In more complete terms, it can be stated this way: Are we placing too much trust in the systems managers who run our nation's medium- and large-size computer systems?

I am posing this question for a practical reason, not a theoretical one. Lost in the furor over the mass electronic break-in is the fact that it could have been prevented - if the people in charge of the computers had been doing their job.

The hacker, Robert Morris, exploited a weakness in the operating system of these computer systems. The weakness was known to the operating system's designers, and the company that supplies the operating system had long ago sent notices to all its customers explaining how to patch the operating system to fix the weakness.

All these thousands of systems managers had to do was read their mail.

Most of them didn't. Most of them ignored the plea from the operating system's designers to make the fix before someone broke into these computers through this weak area, called the "back door."

There is no other word for this than incompetence. Those who think it's unlikely that most mainframe computer systems managers are incompetent - at least in this one area, if in no other - have their heads in the sand.

Think of it in terms of human viruses. If doctors throughout the country were warned of a potentially dangerous weakness in a major drug and most of them did nothing about it, how forgiving would we be? We would demand that the medical profession act immediately to remove those doctors who don't have enough sense to protect the public.

Are we going to do the same thing in regard to our systems managers?

I'm a realist. I know what the answer is. They'll go on protecting their jobs by making up excuses. They'll tell the people who hired them that the entire subject is too technical to explain, but they have the situation well in hand.

Bull. Every systems manager who ignored the warnings on the flaws in Unix, the operating system that Robert Morris sailed right through, should be fired.

It's as simple as that. It's time that we treated networked computer systems seriously. It's time that we stopped accepting the technobabble from these incompetents as something that no one else can comprehend. The rest of us can comprehend it just fine, thank you.

If you agree, mail a copy of this column to your boss. Send a copy to the person who hires and fires the systems manager in your company or university.

Send 'em a message before another Robert Morris sends them something else.

* * *

How can computers catch a virus?

It's easy.

Keep in mind that a computer works quite a bit like a human being. Both need a central processor to run properly - a CPU chip in one case and a brain and central nervous system in the other. And both need the correct programs to work right - an operating system in the computer and an autonomous set of instructions to the organs of the body in the human.

Each one can get sick when a virus works its way into the system and throws it off stride. In both the computer and the human, the virus hides itself and alters the day-to-day operations of its host.

In its mildest form, the virus merely slows everything down. The computer responds sluggishly, and the human feels weak and rundown. At its worst, the virus can make either type of host so sick that it may not recover without intensive care.

So far, what we have been describing also characterizes a simpler form of intruder, called a worm. The difference between a worm and a virus is that worms don't create new copies of themselves, but viruses do; in fact, the strongest viruses in computers and humans can create new clones of themselves many times a minute.

The major conceptual difference is that human viruses are actual creatures, and they can sometimes be seen under a microsope. But computer viruses are formless groups of numbers written as a program. This may make them seem less harmful than human viruses, but it would be a serious mistake for us to treat them that way.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 81

Monday 21 November 1988

Contents

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

Computerized voting problems in Toronto

Amit Parghi <aparghi@watcgl.waterloo.edu>
Sun, 20 Nov 88 18:13:44 EST

From _The_Globe_and_Mail_, Saturday, 19 November (reprinted w/o permission):
Machine misses 1,408 votes, Toronto clerk wants recount by Sean Fine

Toronto's city clerk is asking council to order a city-wide recount after 1,408 votes in Monday's [14 Nov.] civic elections went unread by sophisticated new machines. [...] "We want the integrity of the election to be upheld," deputy clerk Barbara Caplan said in explaining why all 16 city wards, plus the

Metro Toronto wards and trustee races, should be retabulated. Ms Caplan said the recount could affect the outcome of only one city race, the three-vote victory for reformer Malcolm Martini over conservative Michael Walker in Ward 16. As well, three school trustee races could be affected.

But a battle may occur over the manner of the recount. The clerk's office wants to give the machines, purchased recently at a cost of $1.6 million (Canadian), another chance. Ms Caplan said the computerized vote-counting machines were not to be faulted. An error in the printing or cutting of ballots put them "off- register," or off-line, meaning they could not be scanned by the machine, she said. In the recount, those ballots that are not read by the machine would be tabulated manually, she said. [...]

In the city's closest race, which pitted Mr. Walker against Mr. Martini, Mr. Walker, a six-year veteran of council, was initially declared the victor Monday night. On Wednesday, the clerk's department discovered errors in manual addition and Mr. Martini emerged the winner by three votes. Now the entire ward race is in question since 81 ballots were not read by the machine. [...]

In no other city ward, and in none of the eight Metro wards located in the City of Toronto, was the margin of victory smaller than the number of unread ballots. The number of ballots not read ranged from a low of 47 in Ward 4 to a high of 237 in Ward 12. [...]

Under law, the ballots would have to be read in the same fashion - that is, by the machines - as on election day, Ms Caplan said. Only those ballots rejected by the machines would be read manually.

NH State Republican Convention Computerized Voting Standard Resolution

Have Rdb Manuals -- Will Travel 264-3839 MKO1-1/B02 <hyde%isws23.DEC@decwrl.dec.com>
Mon, 21 Nov 88 12:32:19 PST

The following resolution was the only proposed resolution which passed at this year's New Hampshire State Republican Convention:

WHEREAS The State of New Hampshire has set no minimum standard for computer security in computerized voting, and

WHEREAS The state of the art in computer crime has progressed dramatically in the last few years to now include virus programs which can transmit themselves from one computer to another without active participation by the computers' owners, operators, or users, and

WHEREAS The State of New Hampshire has computerized voting equipment, some of which:

- o Does not have the ability to recount manually,
- o Does not have the ability to recount at all,
- o Uses secrecy of internal procedures as a primary security strategy,
- o Does not give the voter the ability to ensure the computer has voted as instructed,

> NOW THEREFORE, BE IT RESOLVED that the Republican Party of the State of New Hampshire calls upon the Legislature of the State of New Hampshire to enact legislation that would establish the following minimum computer security features for any further expansion of computerized voting or vote counting:
>
> > Computerized voting equipment must either produce a manually recountable ballot for the voter's inspection prior to electronically casting the voter's ballot or use as its input a ballot which can be used in a manual recount.

Submitted by Kurt Hyde, Delegate from Weare.

This proposed standard is essentially the same one proposed at the first National Symposium on Security and Reliability of Computers in the Electoral Process at Boston University in August of 1986 (Co-chaired by Eva Waskell and myself).

Many thanks to the RISKS Forum members who participated in the development of this standard during 1985 and 1986.

Kurt

Ethics

Hugh Miller <MILLER@vm.epas.utoronto.ca>
Wed, 16 Nov 88 23:39:09 EST

Stan Stahl, in RISKS 7.75, writes:

> The critical bottom line, and it is one that shouts out to us in the
> wake of the RTM worm, is that we absolutely must begin to take the
> teaching of ethics seriously. Some school districts are beginning to do
> this and they are to be commended for it. Perhaps if everyone were
> exposed to ethics courses, beginning in the early grades and continuing
> through computer ethics courses and business ethics courses, etc, then
> it would be clear `in the entire community what is and what isn't
> ethical behavior.'

In my experience teaching ethics here and at McGill University, such courses have little direct effect on the moral behaviour of the students taking them. About all that can be expected -- and this is the *maximal* result -- is that the students will be made aware of one more set of constraints they must operate within: a code of professional ethics. (In those states which permit them. Many don't.) Like all such codes, the extent to which they are taken seriously has much more to do with upbringing, personality, generally accepted broad social norms, peer pressure, etc., than with schooltime pedagogy. Clever people, or persons thinking themselves above or outside the rules, always find excuses for circumventing them. Scientific pursuits in general, and mathematical/logical ones in particular,

due to the glamour and the cachet of difficulty attached to them, encourage adepts in such beliefs. The famous technological imperative is at work as well: do what is "technically sweet" first, and ask whether it was good after all once it's done. The novelist Walker Percy in one of his books quotes "a scientist's prayer, if scientists ever prayed, which they don't: `Lord, grant that my work lead to the betterment of the human condition, and not the reverse. Failing that, Lord, let it not lead to the complete destruction of mankind. And, failing that, Lord, please don't let the end come before my article is published in *Brain*.'" And, frankly, the general culture we live in worships at the altar of Expediency, not Justice or Virtue, so one cannot expect much help there.

Further, most `ethics' instruction at the university level with which I am familiar proceeds along lines so shallow and analytical that it completely fails to engage the spirit of the listener. One doesn't have to be a devotee of Allan Bloom or his ilk to see this. However dedicated and forceful the teacher, the material taught is so unchallenging and `conservative' (in the sense of supporting the *status quo*) that even the very young see through it and hit their mental channel-changers. To explain why this is so would require a long discussion, descending occasionally into rant and tirade, of the practice of moral philosophy in the English-speaking world in the 20th century, the which I will spare us all. Suffice it to say, the first ethics course most students take is, in my overwhelming experience, the last.

This is not to say that I oppose teaching ethics. Obviously, if such teaching does nothing more than lower the rate of mischief in general circulation by a little bit it is A Good Thing. I merely wish to point out the limitations of all such pedagogy. The teacher in *Stand And Deliver*, please note, was NOT teaching ethics.

Hugh Miller, University of Toronto, MILLER@UTOREPAS.BITNET

Re: Teaching "Ethics"

Brint Cooper <abc@BRL.MIL>
Thu, 17 Nov 88 11:58:50 EST

Eric Roskos writes,

> In an Ethics course, the most you can do is discuss ethical paradigms, which
> include systems of ethics in which it is entirely acceptable to engage in any
> activity that benefits you ("situation ethics" are an example of this).

We're missing something in this discussion. A few digests back, someone observed that post-Watergate attorneys began taking ethics courses as part of their training. But I don't believe for a moment that the purpose was to "teach" ethics to the attorneys. It was simply to get on the record that the attorney had studied ethics so that he could not later claim ignorance of

ethical concepts or their irrelevance to his/her professional conduct. By this, ethical considerations can now legitimately be raised in disciplinary proceedings.

It may come down to this in Computing Science as well.

_Brint

Decompiled Source (Re: RISKS-7.79)

Phil Karn <karn@ka9q.bellcore.com>
Thu, 17 Nov 88 13:02:35 EST

Some argue that the decompiled source code to the Internet worm shouldn't be released because that would make it easier for someone to turn it into something really damaging.

This is a specious argument. Anyone can modify the worm's object file into something very malevolent, and it doesn't even require the use of adb. Just write an exit() that actually does "rm -rf /" followed by an infinite loop, and link it to the worm object file using ld -r so it can be the subject of another ld run. I simply refuse to believe that I'm the only person to think of something like this.

The only "sensitive" information contained in the worm source is the security holes it exploits, and these are now very widely known. The worm is completely powerless without them, and you don't need the worm to exploit in much worse ways a system that still has the holes. On the other hand, there are a lot of people who have perfectly legitimate reasons for wanting to see that code. I, for one, would very much like to show my management and our security staff exactly what it did (*and* did not) do. Although I personally have no reason to believe that the analysis prepared at MIT and Berkeley is not complete, it is just not the same thing as having the actual source in hand when trying to reduce the general paranoia level in others.

Phil

Re: Risks of unchecked input in C programs

<attcan!utzoo!henry@uunet.UU.NET>
Sat, 19 Nov 88 00:22:36 EST

A small error of fact in Bill Stewart's contribution:

>I've always been dissatisfied with the printf/scanf family - field widths are
>hard-coded in the format strings, with no way to parameterize them except
>building format strings on the fly...

Not true, and it hasn't been true for a long time. A field width or precision specification of '*' means "pick up an integer from the parameter list at this point". Either Bill has a very strange version of Unix or he just missed this in the manual page -- it's been there at least since V7,

which came out nearly ten years ago.

Henry Spencer at U of Toronto Zoology
uunet!attcan!utzoo!henry henry@zoo.toronto.edu

Smart Roads

Robert Brooks <rb%hpda@sde.hp.com>
Fri, 18 Nov 88 15:35:22 pst

Many articles have appeared recently about "smart roads"; systems in which communication of some sort between roads and vehicles enable such things as automatic toll assessment, route planning, traffic jam avoidance, etc. Much concern has been expressed about the Big Brother potential of such systems. But this is by no means an essential hazard. The transponders, barcode tags, or whatever could be purchased anonymously, and authorization to cross various toll points n times purchased in advance, like postage stamps. Attempting to pass without prepaid authorization triggers a buzzer, light, gate, or something directing one to a conventional toll booth. Those who proceed anyway are chased down like someone who goes through an ordinary toll booth without paying.

Any technological advance is greeted by cries of "it won't work" and irrational fears. Smart roads are no exception. We should indeed protest implementations of the technology which are invasive to privacy, but suppress Luddite urgings to abandon it altogether.

IFF & UK Toll Roads

Nigel Roberts, G4IJF <roberts%untada.DEC@decwrl.dec.com>
17 Nov 88 17:25

IFF (Identification Friend or Foe) and Toll Roads in the UK

Fitting IFF to cars

Chaz Heritage and others raise genuine concerns about the possibilities for intentional and unintentional misuse of such a hypothetical system.
However I do feel some of the more fantastic possibilities are unlikely to materialise. (Of course other risks, maybe with even worse consequences than already imagined might, so don't stop discussing this!)

European Single Market

From 1992, all goods sold in the Single Market must conform to common specifications. As a result, National Type Approval for cars will be replaced by a type approval for the whole of the EEC. (This, in fact will apply to all goods & services, but we are discussing cars here)
For example, the U.K. would like to introduce a requirement for U.S. style third brake lights. However before it can do this, it needs all the other member countries to agree.

So to REQUIRE the fitting of an IFF-style device, it must be agreed by all the EEC countries (and it must then conform to a common standard).

The British consumer may in its lethargy accept Big Brother, but here in W. Germany there would be a revolution if such an intrusion into privacy was even so much as suggested. (There was enough outcry when machine-readable passports/national ID cards were introduced; this was somewhat pacified by removing the requirement to carry I.D. at all times)

Foreign Vehicles

The number of foreign registered (usually European) vehicles on British roads is increasing all the time, with the increase in contacts, trade, etc, with the mainland which has occurred since the U.K. joined the EEC in 1973.

When the Chunnel opens there will be even more.

The U.K like most countries. is bound by the terms of the Treaties on International Road Traffic to let visitors to the U.K. drive on their roads. If the Essex Police got a MAIL message every time a car without a U.K. IFF plate drove along the A12 (a major 'E' route) then their computer systems would soon be overloaded.

Simple ways are best

As a final postscript on the theme of "Big Brother is watching you"; let me ask the rhetorical question:

"Why use complicated methods of control when simple ones are best?".

An example: all vehicles loading on to one particular ferryboat are monitored by video as they pass Passport Control.
Presumably, during the crossing, a list of all license plates can be made, and telexed across to the destination port.
What could be simpler than that? Why use complicated electronics when old-fashioned surveillance works just as well, if not better.

Nigel Roberts

Re: "Electronic number plates"

Allan Pratt <imagen!atari!apratt@ucbvax.Berkeley.EDU>
Fri, 18 Nov 88 14:40:59 pst

I saw a segment on "Electronic number plates" on "Beyond 2000" (or "Towards 2000"), a series from Australia which actually goes into more detail than most shows... They start with the Big Picture, but they don't stop with "but now it gets so complex you couldn't possibly understand it" -- they go on to explain in some technical detail.

So here's what they said: The "black box" is welded to the frame of your car, and is virtually indestructable. It has no external features. It has no power source (!). If the handshake fails, a camera snaps a

picture of car, driver(?), and traditional number plate.

The system they showed had 10 (?) nodes in central Hong Kong (or some other high-density Asian city). There are still a few bugs to work out of the system, which RISKS readers have been quick to point out.

No power source? I guess part of the inquiry from the roadbed is energy enough for it to transmit back.

Towards 2000 and Beyond 2000 are on The Discovery Channel, which cable services sometimes have as part of the basic service.

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

---

Re: UK vehicle-identification systems

<att!ihlpl!jhh@ucbvax.Berkeley.EDU>
Mon, 21 Nov 88 08:03:05 PST

denbeste@OAKLAND.BBN.COM writes:
>I find Chaz's description of the new system in Britain for toll-roads very
>interesting, to say the least. I have some interesting questions:

>1. As I understood it, what we have is a radio handshake between each car and
>fixed transceivers at the entrance and exit from the toll-road, presumably
>connected to a computer billing system which mails you a bill each month. What
>if you move and don't tell the computer your new address?

The Illinois Toll Authority has already installed this automated toll collecting equipment on one exit as a trial. They are retaining the coin collection equipment, but are also supplying several large users, such as limousine services and trucking companies, who use this exit with equipment that will allow the users to be billed directly. The device can read the identification of vehicles traveling at up to 35 MPH [56 km/hr]. Since the coin collection boxes are located on a curve here, the speed limit should pose no problems. In case you are from the Chicago area, this equipment is located at the Farnsworth exit off of the East-West Tollway, I-88, formerly IL-5. Unfortunately, there was no information readily available to describe the transceiver.

The Illinois Toll System does not use entry/exit tolls, but rather periodic toll barriers. This causes large backups during rush hour, as everyone has to put in their $0.40. The hope is that this system will reduce congestion, and that the expense of adding more toll booths can be avoided.

John Haller jhh@ihlpl.att.com

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 82

Wednesday 23 November 1988

Contents

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

Troubles with automatic vote counting in Toronto

Mark Brader <msb@sq.sq.com>
Tue, 22 Nov 88 15:00:59 EST

[Background: In Canada, voting in all levels of election has been done by the voter pencilling an X on a paper ballot, which is then counted by hand. Municipal elections are normally the only ones where multiple offices are voted on at once, with several X's on the ballot.

In Ontario, all municipal elections are synchronized and they were held last week. For the first time, the elections in Toronto used an auto- matic

technique. The voter had to blacken a circle to vote for a candidate; obviously optical mark recognition.]

Toronto Star, November 22, 1983:
Toronto is going to make doubly sure that a recount of last Monday's municipal election ballots is correct. At an emergency meeting of the outgoing city council yesterday, politicians ordered staff to recount all 142,107 ballots by hand as well as by automatic voting machine -- an arduous task that could take several days.

Although provincial law only recognizes the machine count, councillors said the unofficial manual recount will [!] help to restore confidence in the city's new $1.6 million automated system.

The recount was recommended by City Clerk Roy Henderson last week after his staff discovered that a record 1,408 ballots were rejected by the city's new automated voting machines. The machines are programmed to reject spoiled ballots, but Henderson says he finds "it hard to believe that there were 1,408 spoiled ballots".

Because the rejected ballots were not singled out when they were initially fed through the machines [sigh!] on Monday, a recount is needed to find the rejected ballots and examine them, he told council.

Henderson said he believes that the high number of rejected or "unread" ballots was not the fault of the machines, but due to a cutting error on the ballots. Staff ran some ballots through the machine as a test last week and found that some ballots were not cut properly, but correctly filled out, were rejected, he told council.

"Any variance of 25 thousandths of an inch would cause the machine to reject a ballot", he said, quoting information from the Business Records Corporation, the American company that supplies the city's voting machines and ballots.

The only race in Toronto that could be affected and which wasn't already so close that recounts had already been called is the contest for public school board trustee in Wards 9 and 10. Sandra Bussin beat Anne Ferguson by 217 votes, but the number of "unread" ballots in those wards was 238.

... Some alderman questioned why the city should do a full recount of all the wards if the outcome of the election won't be changed and staff already know what caused the error.

"The electorate has to be confident that the vote tabulation machines do the job they are supposed to do", city solicitor Dennis Perlin replied.

[There were no such reports of problems from other municipalities in Metropolitan Toronto which also used the voting machines.]

Mark Brader, Toronto utzoo!sq!msb, msb@sq.com

Risks of remote registration

Mon, 21 Nov 88 21:44:24 PST

"Touchtone registration" is what many universities are going to, including the one I work for. This allows students to register, drop, and add classes from the comfort of any available touchtone phone. (There are some on campus for students that don't have access to one normally.) Unlike the previous early registration system, it allows students to choose their own alternatives when classes are filled or are not allowed. (class full, conflicting times, not authorized, etc.)

What worries me is the choice of 9 digit student ID (one will be assigned in the 900 range for students not supplying their SSN) and 6 digit access code (the student's birthday). With this information about any student, it is possible to rearange their schedule. (Confirmation of the change is sent in the mail, assuming that your address is up to date.) Pranks (register someone for "human sexuality") and dropping someone from a full class so you can get in are possible abuses, as is changing your mind about a schedule rearrangement then complaining that you didn't do it.

[Supposedly, ethically minded students would not entertain such pranks? But, historically, pranks abound among college kids. On the other hand, designing a system to prevent such malicious misuse is not easy. Note that audit trails would not help much, because the record will say that the victim was the person who authorized the change! A written notification might help, with some period allowed for appeals that it was not legitimate, but that too could be abused intentionally -- e.g., to give you a deferred option... PGN]

Computer Breakin article

"Maj. Doug Hardie" <Hardie@DOCKMASTER.ARPA>
Wed, 23 Nov 88 13:56 EST

The following is taken from Intercom, Vol 28, No 24, Nov, 11, 1988, an Air Force Communications Command newsletter:

Computer break-in

By Special Agent Mike Forche, AFOSI computer crime investigator

A computer hacker penetrated an Air Force Sperry 1160 computer system in the San Antonio, Texas, area. The hacker was discovered by alert Air Force Communications Command computer operators who notified the data base administrator than an un-authorized user was in the system. The data base administrator was able to identify the terminal, password, and USERID (system level) used by the hacker.

The data base administrator quickly disabled the USERID/password (which belonged to a computer system monitor). The data base administrator then observed the hacker trying to get into the system using the old USERID/password. He watched as the hacker successfully gained entry into the system using another unauthorized

USERID/password (which was also a system administrator level password).

The hacker was an authorized common user in the computer system; however, he obtained system administrator access level to the government computer on both occasions.

Review of the audit trail showed that the hacker had successfully gained unauthorized access to the computer every day during the two weeks the audit was run. In addition, the hacker got unauthorized access to a pay file and instructed the computer floor operator to load a specific magnetic tape (pay tape).

The hacker was investigated by Air Force Office of Special Investigation computer crime investigators for violation of federal crimes (Title 18 US Codes 1030 computer fraud, and 641 wrongful conversion of government property), Texas state crimes (Title 7, Section 33.02 Texas computer crime wrongful access) and military crimes (obtaining services under false pretense, Uniform Code of Military Justice, Article 134).

The computer crime investigators made the following observations:

- USERIDs used by the hacker were the same ones he used at his last base when he had authorized system access in his job. The use of acronyms and abbreviations of job titles will hardly fool anyone; plus the use of standard USERID base to base is dangerous.

- The passwords the hacker used were the first names of the monitors who owned the USERIDs. The use of names, phone numbers, and other common easily-guessed items have time and time again been beaten by even the unsophisticated hackers.

The risks of using CACM inserts

<hughes%math.Berkeley.EDU@cartan.berkeley.edu>
Tue, 22 Nov 88 22:05:29 PST

In the November 1988 issue of CACM, at page A-17 there is a tear-out postcard for ordering ACM Press book. On the back of the postcard there is a blank for one's credit card number and expiration date.

Yes, on a postcard.

Eric Hughes hughes@math.berkeley.edu ucbvax!math!hughes

ETHICS AND SOFTWARE

Ezra Zubrow <APYEZRA@UBVMS>
Mon, 21 Nov 88 16:46:00 EST

From: IN%"KAHIN@hulaw1.HARVARD.EDU" "Brian Kahin 617-864-6606" 18-NOV-1988

17 : 5 3

Return-path: info-law-request@sem.brl.MIL
Date: Tue, 15 Nov 88 16:36 EST
From: Brian Kahin 617-864-6606 <KAHIN@hulaw1.HARVARD.EDU>
Subject: EDUCOM white paper

Readers of this list may be interested in the white paper, "Property and Propriety in the Digital Environment: Towards an Examination Copy License," just published by the EDUCOM Software Initiative. The paper, which I prepared for ESI, proposes to two model licenses to encourage faculty evaluation of software programs while maintaining respect for the rights of copyright owners.

The first model license is for "circulating evaluation copies" -- i.e. copies which can be circulated by libraries or other campus facilities. It is targeted to commercial publishers of tools and courseware.

The second model license is for "distributable evaluation copies" -- copies which may be downloaded or duplicated subject to certain conditions. In effect, it proposes a standard for "academic shareware" that is more rigorous than conventional shareware licenses. It addresses the differences among shareware licenses by offering a kind of lowest common denominator. It is hoped that the model license -- and the kind of user environment that the EDUCOM Software Initiative is trying to foster -- will encourage academic authors to disseminate evaluation versions of their software over the academic networks.

The white paper will appear in the next issue of the EDUCOM Bulletin. A specially published version is available on request from the EDUCOM Software Initiative:

EDUCOM Software Initiative, PO Box 364, Princeton, NJ 08540 609-520-3340
BITNET: esi@educom

Teaching Children Ethics

"Homer W. Smith" <CTM@CORNELLC.ccs.cornell.edu>
Mon, 21 Nov 88 23:05:40 EST

There is much apathy about teaching ethics to our children. Some have suggested this is because the ethics that is being taught is really only in the self interest of the teacher at the expense of the child. 'It is your DUTY to die for your country whenever the government calls', etc.

Others have suggested it is because religions of various sort have given it a bad name by making ethics some sort of absolute code of behavior independant of any external circumstances. If you are married and there is an atomic war and you and someone else who is NOT your wife are the only two people left alive, is it immoral to have sex with them to restart the human race even if there is no preacher to marry you?

Maybe there is something to be said for these ideas that years of misuse of teaching ethics for ulterior motives has given it a bad taste in everyones mouth, but it seems to me that there is still away to revitalize the subject as long as we leave the religious fanactics and the parents telling their kids its unethical to talk back out of the picture.

One of the most effective ways of teaching new drivers to slow down and drive carefully is to show them movies of mangled corpses from accidents. Sometimes movies are not enough. After having seen a few real cars that had been wrapped around a telephone pole, I got a message through to my brain about something or other that I will never forget. Cars are fragile and should be driven with care.

Maybe by indoctrinating kids with the RESULTS of unethical behavior in its goriest details and letting THEM decide and vote on how it came about and what was unethical and how to avoid it, we will form young adults who are capable of determining ethics for themselves from the data of the consequences. Show them the consequences and let them figure it out, rather than tell them the answer (what is and is not ethical) and hope they never have to see the consequences.

How many kids develope sexual tragedies (pregnancy, disease etc.) because their well meaning (?!) parents never talked to them about sex for fear they would HAVE sex if they knew about it. Are we not ALL suffering from this kind of mentality in America today?

Christ, kids don't WANT to hurt. Don't you think we can solve the teaching problem just as we have solved so many others? Some would tell you that people are bascially bad, certainly seems this way sometimes. Maybe people look into their own hearts and they see THEY are basically bad so they teach that others are also. But maybe this is all wrong. Maybe people are basically GOOD. Even bad people. Maybe something went wrong. Maybe it is up to us to figure it out and do it right.

The solution to apathy is to realize that there IS a problem, and there IS an answer, and WE WILL find it. You just keep going until you do. The only other answer is to lock everyone up at birth.

Homer W. Smith
Senior Programmer
Hubbard Fractal Research Facility
Cornell National Supercomputer Facility

Re: toll road speed checking

Brent <brent@itm.UUCP>
22 Nov 88 14:05:48 GMT

Pennsylvania has been using entry-exit tolls on the Penn Turnpike for a good many years now. One of the main problems they ran into when they first cut over about a decade ago hasn't been mentioned here yet: Unsynchronized clocks. That's right. There was no "master clock" for all the toll booths. The problems are obvious. On short trips you found yourself exiting *before*

you got on (does this mean they pay YOU a toll?) or on medium-length trips, it was common to average somewhere over 400 miles per hour between two certain booths. This was during the era of mechanical clocks, but such problems could easily carry over to the electronic age.

brent laminack (gatech!itm!brent), In Touch Ministries, Atlanta, GA

Privacy vs UK vehicle-identification systems

Andrew Klossner <andrew@frip.gwd.tek.com>
22 Nov 88 16:46:36 GMT

> "Why not make use of such a system voluntary? ... The principle seems to me to be that if you are potentially diminishing someone's privacy, they should have a choice about it, and the costs and benefits should be made clear."

In the proposed scheme, people who desire privacy must single themselves out by entering the queue of those who want privacy. This alone diminishes their privacy.

It's similar to a (fanciful) scheme in which voters can choose the "express, no privacy" line, where others can see their choices, or can select a standard voting booth. Those who choose to vote in privacy may be stigmatized as those who have "something to hide."

Andrew Klossner, Tektronix, Wilsonville, Oregon
(uunet!tektronix!hammer!frip!andrew) [UUCP]

RightTouch service

Scott C. Crumpton <NESCC@NERVM.NERDC.UFL.EDU>
Wed, 23 Nov 1988 09:12:05 LCL

The following blurb along with a flyer appeared in my phone bill yesterday (Upper/lower case added by me):

> Suspend, restore and disconnect with RightTouch(SM) service
>
> You can suspend, restore or disconnect your Florida home telephone service at your convenience with Southern Bell's RightTouch service. You can use RightTouch service 24 hours a day, seven days a week by dialing 1 800 826-6290 from a touch-tone telephone. There is no additional charge for using the service, although the normal charge for restoring your phone service still applies.
>
> To access RightTouch service, you will need the personal access code (PAC) shown below. This code has been assigned to your telephone number and should be protected as you would a credit card.

Personal access code xxxx

Once you dial the RightTouch service number, easy-to-follow verbal instructions will guide you through the ordering processing to suspend, restore or disconnect your phone service.

Yet another 'service' I can do without, but there's a positive side to this one. It's currently possible to initiate some types phone company service orders via a simple verbal phone call. No significant attempt is made to identify that the caller is who they claim to be. If RightTouch eventually *replaces* that process then it may actually be an improvement. It depends on how well it handles repeated invalid password attempts. ---Scott.

Cordless Telephones

<walker@ficc.UUCP>
Mon Nov 21 14:28:06 1988

Last week I purchased and installed a cordless telephone. It is marketed as the "Freedom Phone" by Southwestern Bell (the local AT&T spinoff). After one phone conversation, I noticed that, for a very brief interval, I could hear what sounded like another conversation. I've experienced cross-talk on long-distance calls, but this was a local call. Anyway, I suspected that I was hearing another cordless telephone.

To verify this, I unplugged the base unit (to kill its carrier signal), and, by golly, I could hear *both ends* of on of my neighbor's phone conversations (I recognized my neighbor's voice!) I checked the manual to see what to do about this - after all, if I can hear my neighbor, couldn't he hear me? The "Freedom Phone" transceiver uses any one of 10 channels in the 46-49 MHz range, selectable by an internal rotary switch. Well, I switched the handset to each of the 10 possible channels, and could hear conversations on EVERY CHANNEL!

The unit has a 9-bit "security" DIP-switch, but this seems to only prevent another handset on the same frequency from accessing my base unit.

The unit advertises a range of 1000 ft., and I'm sure that range is for usable access of the base unit. Actual audible signal range appears to be MUCH farther.

When actually using the phone properly, with the handset in close proximity to the base unit, the relative signal strength of the units is much stronger than a neighbor's more distant unit, so you are normally unaware of a neighbor on the same channel. However, when using the cordless phone, I now always consider that others may be listening!

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 83

Monday 28 November 1988

Contents

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

Tech Report on the Internet Worm

Gene Spafford <spaf@purdue.edu>
Mon, 28 Nov 88 19:53:07 EST

My tech report on the Internet Worm is finally finished! You can get a compressed PostScript version of the formatted report via FTP as follows:

1) ftp to arthur.cs.purdue.edu (128.10.2.1)
2) login for anonymous ftp
3) set binary mode on
4) cd pub/reports
5) get TR823.PS.Z
6) quit

Then uncompress the file and print it.

[If you cannot uncompress it, you may access the UNCOMPRESSED PostScript file directly (280,827 bytes, by the way!):
OMIT 3) above; it should also work in binary mode, but more slowly;
REPLACE 5) above with "get TR823.PS", using the name of the uncompressed PS file. Also, use a copying machine if someone you know has already FTPed it. Spare the Internet. PGN]

If you have already ordered a paper copy of the report and you can FTP a copy to print it yourself, please send me mail and cancel your request for a paper copy.

If you cannot FTP a copy and you have already ordered a paper copy, have patience. As soon as they get printed they will be mailed -- before the end of this week, I am told.

If you cannot FTP a copy and would like to order a paper copy, send me your surface mail address and I will add your name to the list.

Cheers,
--spaf

Tech report on the Internet Worm

Peter Neumann <Neumann@csl.sri.com>
28 Nov 1988 18:59:19-PST

Spaf's ``The Internet Worm Program: An Analysis'' is an extremely thoughtful and comprehensive report. It will be standard reading for years. It is offered by Spaf ``solely for the purposes of instruction and research'' (as he states in his title-page copyright notice), and is cited in RISKS for precisely those purposes. There are many lessons to be learned -- including needs for better operating systems and network protocols, better quality programmers with greater social awareness, better ethical teaching, better laws, and generally better understanding of THE RISKS. Our thanks to Spaf for his considerable contribution. PGN

Congress plans hearings on the Internet Worm

<jon@june.cs.washington.edu>
Mon, 28 Nov 88 09:35:59 PST

The House Science, Space and Technology Committee and the House Judiciary Committee are planning hearings on the Internet virus for the upcoming 101st Congress.

Also, the author of the federal computer crime law says that he believes the virus programmer could be prosecuted under that law. Here is the source, from a story that appeared in THE SEATTLE TIMES, Sunday Nov 27 1988, p. B2:

CONGRESSMEN PLAN HEARINGS ON VIRUS - Newhouse news service

WASHINGTON - The computer virus that raced through a Pentagon data network earlier this month is drawing the scrutiny of two congressional committee chairmen who say they plan hearings on the issue during the 101st Congress.
Democratic Reps. Robert Roe, chairman of the House Science Space and Technology Committee, and William Hughes, chairman of the crime subcommittee of the House Judiciary Committee, say they want to know more about the self-replicating program that invaded thousands of computer systems.
The two chairmen, both from New Jersey, say the are concerned about how existing federal law applies to the Nov. 2 incident in which a 23-year-old computer prodigy created a program that jammed thousands of computers at universities, research centers, and the Pentagon.
Roe said his committee also will be looking at ways to protect vital federal computers from similar viruses.
`As we move forward and more and more of our national security is dependent on computer systems, we have to think more about the security and safety of those systems,' Roe said.
Hughes, author of the nation's most far-reaching computer crime law, said his 1986 measure is applicable in the latest case. He said the law, which carries criminal penalties for illegally accessing and damaging `federal interest' computers, includes language that would cover computer viruses.
`There is no question but that the legislation we passed in 1986 covers the computer virus episodes,' Hughes said.
Hughes noted that the law also includes a section creating a misdemeanor offense for illegally entering a government-interest computer. The network invaded by the virus, which included Pentagon research computers, would certainly meet the definition of a government-interest computer, he said.
`The 1986 bill attempted to anticipate a whole range of criminal activity that could involve computers,' he said.

Computer Literacy #3

Ronni Rosenberg <ronni@juicy-juice.lcs.mit.edu>
Mon, 28 Nov 88 12:36:39 EST

Expenditures of time and money on computer-literacy education represent important tradeoffs for schools. If you think that computer literacy should be taught in school, how do you think schools should pay for it (hardware, software, training, maintenance)? How should computer-literacy courses be fit into the school day?

Since school budgets and days are finite, these questions raise the issue of priorities. Should computer-literacy education be a high priority for our education system? Why or why not? How do you compare computer literacy with current education priorities?

[Respond to Ronni, please. PGN]

More on misuses of computers

Peter Neumann <Neumann@csl.sri.com>
28 Nov 1988 17:17:10-PST

A flurry of risks relating to antisocial computer uses has been rapidly developing into a blizzard:

* Hatred-promoting materials. Jeff Stout (jstout@boeing.com) alerted me to an article in the Seattle Times/Post-Intelligencer, 11/20/88, excerpted as follows:

> The rapid spread in recent months of illegally produced floppy disks with anti-Semitic and racist content, promoted by the increased use of home computers, has alarmed West German teachers and those concerned with protecting young people from exposure to military, racist and pornographic violence.
>
> The neo-Nazi underground has changed tactics", says Gerhard Adams, deputy chairman of the government office responsible for monitoring "youth-endangering" materials. "Instead of distributing leaflets, they now circulate in schools computer programs which are anti-Semitic and racist." [...]
>
> While the majority of games glorifying war and Rambo-style episodes of self-enforced law are produced in the United States and Great Britain, games inciting racial hatred and propagating Nazi ideology are believed to have their origin in Germany.

* A flurry of PC porno programs (including some highly interactive versions). For example, a porno program is apparently sweeping through the banking community (Lounge-suit Larry ...), some versions of which are Trojan horsed and rather destructive. Many others have also been reported, and with pirating and direct propagation seem to be spreading rampantly.

* Electronic chain letters such as that noted in the following message.

So, what is new? The subject matter is certainly not new. But the medium offers new opportunities -- proliferability, programmability, and privacy. (Next we will be having subliminal messages on the screen, or even buried inside the programs?)

Chain letters = next net disaster ?

Ira Baxter <baxter@madeleine.ICS.UCI.EDU>
Fri, 25 Nov 88 23:37:04 -0800

Just received this. Figured best way to a) satisfy RISKS readers and b) "prevent breaking the chain" :-} was to submit this rather than victimize 20 more people. If this sort of thing is turned loose in email, the resulting exponential explosion could be as bad as the recent net worm (with willing vectors, anyhow). Unwilling vectors will just damp them out... but with 3 million PCs out there, how many do we need to keep it alive?

[RISKS has no difficulty whatever in breaking this chain. Chain letters are bad enough via SnailMail, but electronically they open up horrible possibilities. PGN]

Computerized Parking Meters

James Peterson <peterson@sw.MCC.COM>
Mon, 28 Nov 88 16:40:05 CST

While visiting the University of Oregon last summer, I found a parking space with no meter, but a sign directing me around the corner. There was a small terminal with a map of the adjacent parking area, about 14 spaces along the side of the street. The instructions indicated that the money was to be deposited and the code number for my parking space keyed in. Out popped a little printed ticket with my parking space number and the time, date, etc when I arrived and how long before my parking expired. It's the only time I've seen such a system (instead of the normal mechanical parking meters).

I assume the benefits of the system are that there is a centralized station for checking what cars are legally parked (the meter maid doesn't have to check each spot, but one central location), central collection of money, and if one car pays for an hour but leaves after 10 minutes, there is no visible record allowing the next car to just use the remaining 50 minutes without paying for it.

Data verification

Rob Gross <<GROSS%BCVMS.BITNET@MITVMA.MIT.EDU<>
Mon, 28 Nov 88 20:58 EST

At Boston College, most faculty members are expected to advise between ten and twenty students. For various reasons (students requesting new advisors, faculty members on leave, students changing majors), the students I advise one semester often are not my responsibility by the time the next semester rolls around. So I wasn't too surprised when I received a call from a student I had advised in September asking for an appointment to see me; I told her that she was no longer one of my advisees, and suggested that she call the dean to find out who her advisor was.

She called back an hour later and told me that she had been entered into the computer as class of 1993, and the computer had duly scheduled her to register in November of 1989.

And my computer science students worry about why I stress data verification!

Rob Gross

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 84

Tuesday 29 November 1988

Contents

- "Program Verification: The Very Idea", by J.H. Fetzer
  Nancy Leveson et al.
- Internet Worm Tech Report
  Gene Spafford
- Purchasers of computer systems as causes of the Internet worm
  Brandon S. Allbery
- Bank of America ATMs Hit a Glitch
  PGN
- Corps of Software Engineers?
  Henry Spencer
- Software Uniformity Legislation
  Colin M Thomson
- Zapping shoplifters in Minnesota
  Scot E Wilcoxon
- (Counter-)corrective control systems
  Jeffrey R Kell
- Info on RISKS (comp.risks)

"Program Verification: The Very Idea", by J.H. Fetzer

<leveson@electron.LCS.MIT.EDU>
Tue, 29 Nov 88 07:11:44 -0500

In RISKS-7.61, Brian Randell recommended a paper by J.H. Fetzer in the Communications of the ACM vol 31, no 9 (Sept. 88), pp. 1048-1063. There has been no reply in the RISKS Forum, and some people have apparently interpreted this absence as everyone's agreement with Brian's view of the paper. It should be noted, however, that the paper has created great outrage among many in the research community due to its misstatements and distortion of the goals of formal verification, the seemingly low level of knowledge and understanding by the author about formal verification (e.g., misstatements such as the implication that it is only applicable to high-level languages and the lack of references to the verification literature and work of the past 20 years), the inclusion of inflammatory and unsupported statements (e.g., that the practice

of program verification somehow has serious negative consequences ``not only for the community of computer science, but for the human race''), and the general argument that deductive reasoning is not appropriate for computer programs -- which has implications far beyond just formal verification.

Formal, mathematical approaches to system construction and analysis are directly motivated by the concern to construct trustworthy systems -- systems whose developers will be willing to stand before the public and take responsibility for the consequences of their deployment. As yet, this goal is unrealized, but research in formal verification is a serious contribution toward that goal and is both socially and scientifically responsible. Serious and well-informed discussion of the limitations to formal verification, and of its strengths and defects relative to other responsible proposals for the construction of trustworthy systems, is entirely appropriate and would, we are sure, be welcomed by the supporters of formal verification. In fact, many in the field have themselves been the leaders of such discussion (e.g., see the recent discussion by Avra Cohn, ``Correctness Properties of the Viper Block Model'', Cambridge University, England, 1988, regarding her own verification of the Viper microprocessor, and several papers in the book "Mathematical Logic and Programming Languages" that was published on the occasion of C.A.R. Hoare being named to the Royal Society). However, ill-informed and irresponsible attacks upon work that attempts to make computer science a socially-responsible engineering endeavor do not seem to us to be useful or productive.

Mark Ardis, Software Engineering Institute
Victor Basili, University of Maryland
Daniel Craigen, I.P. Sharp
Susan Gerhart, MCC
Donald Good, Computational Logic Inc.
David Gries, Cornell University
Dick Kemmerer, University of California, Santa Barbara
Nancy Leveson, University of California, Irvine
John McHugh, Computational Logic Inc.
Peter Neumann, SRI International
Friedrich von Henke, SRI International

[Other anticipated signatories were not available for final sign-off.]

Internet Worm Tech Report [Risks of Offering Popular Reports]

Gene Spafford <spaf@purdue.edu>
Tue, 29 Nov 88 16:30:12 EST

[In response to a query as to why Purdue FTP stopped working today:]

We're off the air because we had 42 ftp processes running at once, and the ftp daemon got hung. We now need to reboot the machine to clear it, but that means kicking over 100 users off (this is a 10 processor Sequent Symmetry). So, we're waiting until later this afternoon until people have gone home for dinner, etc.

[OK, folks, let's show a little restraint. I picked up a copy in the

off hours yesterday. But FTP FLOOD is clearly just one more denial of service problem that must be anticipated in setting system parameters...

By the way, ALL of the Arpanet/Milnet mail bridges have been today, reportedly due to "technical difficulties". PGN]

Purchasers of computer systems as causes of the Internet worm

Brandon S. Allbery <allbery@ncoast.UUCP>
Mon, 28 Nov 88 21:29:06 -0500

A bit of biographical commentary: I am a consultant and programmer who specializes in systems administration and DBMS systems. This puts me in a position to see how our clients manage their computer systems. For those who are interested, we handle Altos X86 systems, SCO Xenix, and the occasional 3B/2 and even more occasional other small UNIX systems.

I should note that the term "Standard Security Speech" is used sarcastically; insofar as our clients are concerned, it's more of a rant about something that "can't possibly apply to them." It's not written down or otherwise formalized; its content is as variable as the security problems at each client site.

And the context, from the Usenet newsgroup news.sysadmin:

> As quoted from <563@husc6.harvard.edu> by reiter@endor.harvard.edu (Ehud Reiter):
> +---------------
> | I think the vendors bear the lion's share of guilt in this affair.
> | Why the ---- didn't Sun and friends fix these security holes ages ago?
> +---------------

That portion of my response which is relevant to RISKS follows. ++bsa

> --------

I can answer this, perhaps not for Sun but in general.

I've annoyed many a client with "Standard Security Speech #1", discussing the importance of not running all their programs from an unpassworded "root" login. And many of those clients have modems. I didn't realize just how bad the situation was until one of those clients argued back that they bought an ***** (name deleted to avoid advertising) system because a business associate had compained about &&&&'s not allowing "root" to log in on non-console terminals. Why was this so bad? "We don't want to have our users be restricted in what they can do."

The logic of these sysadmins is simple and extremely dangerous: People are ignorant about computers. People don't want security. People want to load their applications into their computers and trust that god will keep the crackers out. And there have been cases when a company will refuse to buy a particular computer because it comes with security enforcement.

The vendors have made mistakes, certainly. But their customers have a nasty

tendency to consider these mistakes to be features. Common arguments used by these people when confronted with the flaws in their reasoning:

"Nobody knows our computer's phone number." -- Demon-dialer programs are trivial, especially when used with smart modems that can recognize voice answers.

"We don't have any information that anyone would want." -- Fine, so you don't have to worry about industrial espionage. This would not have bothered in the least the cracker gang that was broken by the FBI earlier this year, that operated in the Cleveland area [where I live], much less interstate gangs courtesy PC Pursuit or that West German group that used an improperly installed Gnumacs to break into systems.

"It {won't,can't} happen to us." -- Needs no commentary. Ask any sysadmin on the Internet.

Worse is that almost *every* small Un*x system out there has NO security, because the salespeople that installed them and set them up didn't know about it. They have everyone run as unpassworded root. They load applications into /tmp, where any cracker can destroy the entire system with just ONE publicly-executable "rm". They don't say word one about backup procedures. And many of them don't give their customers the master disks to their software, so if their programs get blasted they're gone for good.

That last paragraph is the worst part. We work primarily with reasonably pure Xenix and Unix System V -- no sendmail, no fingerd, no ftpd, no susceptibility to the *current* worm. And capable of quite good security. But setting up security takes some work -- it always has, it always will -- and most salespeople are too busy counting their commissions to consider doing that work. If they even know anything about security, which I would doubt after some of the things I've seen. And even if they did, the people mentioned above would forbid it. (Did I mention the system administrator who told me that he had his people running as root because he didn't want them to be stuck in a restricted shell? No, he didn't mean /bin/rsh.)

The Internet worm is well on its way to becoming the kernel of my "Standard Security Speech #2". Maybe a few people will pay attention this time; one of *****'s failures is that systems ship with a "uucp" login enabled and security disabled even in HDB UUCP. All it'd take is a UUCP version of the Internet worm and a demon-dialer program to wreak havoc in these small systems.

Vendors have some blame, but their oh-so-naively-trusting customers and oh-so-ignorant salespeople (or distributors' salespeople, who the vendors have no control over) have even more. Education is the answer here. It is a sad but true fact that only an actual invasion of their systems will get any response out of them.

Brandon S. Allbery, Telotech, Inc.
Brandon S. Allbery, comp.sources.misc moderator and one admin of ncoast PA UN*X
uunet!hal.cwru.edu!ncoast!allbery <PREFERRED!> ncoast!allbery@hal.cwru.edu
allberyb@skybridge.sdi.cwru.edu <ALSO> allbery@uunet.uu.net
comp.sources.misc is moving off ncoast -- please do NOT send submissions direct
Send comp.sources.misc submissions to comp-sources-misc@<backbone>.

Bank of America ATMs Hit a Glitch

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

A computer malfunction at BoA's main data center appears to have shut down all of the bank's 1450 automated teller machines in California for three hours on Sunday afternoon, 27 Nov 88 (normally a very busy day). The shutdown also affected BofA customers throughout the country. [Source: San Francisco Chronicle, 29 Nov 88, p. C1, article by Kenneth Howe]

Corps of Software Engineers?

<attcan!utzoo!henry@uunet.UU.NET>
Tue, 29 Nov 88 02:02:48 EST

Just noticed in an old Aviation Week editorial (Oct 17):

> "Flexibility is software's strong suit, allowing the military to make changes in how a weapon system functions, even after it is fielded... [discussion of gratuitous changes deleted] ...making changes in a hurry during a conflict is imperative if software is to help US forces prevail."
>
> "Traditionally, armies have had combat engineers to build makeshift bridges, ports, and even airfields in a hurry. But where is the US corp of software engineers that can fix a key software module quickly so the next airstrike can account for an unexpected SAM threat? Do the armed services expect contractor personnel to volunteer for duty on the front lines? Clearly some minimal level of expertise is needed in the field and on board ship to make sure that weapons systems programs can accommodate unexpected circumstances... there is too much riding on software and too little expertise in the military to deal with it."

Henry Spencer at U of Toronto Zoology
uunet!attcan!utzoo!henry henry@zoo.toronto.edu

Software Uniformity Legislation

Colin M Thomson <CMTA@gm.rl.ac.uk>
Mon, 28 Nov 88 16:06 GMT

Conleth O'Connell sent a note to the soft-eng list about US uniformity legislation for software.

I guess there's a risk lurking in there. Either we get legislation appropriate to life-critical software, and all the commercial games outfits go bust, or we

end up with nuclear reactors and flight control systems required to meet mickey-mouse standards. Maybe the legislators will try to classify software, and set up rules appropriate to different sorts of products; if they do, will they get it right?

Tom Thomson, ICL, Manchester M12 5DR, UK
tom@prg.ox.ac.uk cmta@alvey.uk

***** VIEWS EXPRESSED ABOVE MAY NOT CONFORM WITH THOSE OF MY EMPLOYER *****

Zapping shoplifters in Minnesota

Scot E Wilcoxon <sewilco@datapg.mn.org>
29 Nov 88 11:11:40 CST (Tue)

RISKS has already reported on the possibilities of cash registers reporting the purchases of individuals to marketing databases. Some Minnesota stores are now using electronic technology to monitor thieves during individual crimes and at a higher level.

A new superstore recently opened in this area. While reporters were waiting for a demonstration of the security system, an actual theft demonstrated it. In addition to security agents on the shopping floor and the now-common TV cameras, purchases made on the electronic cash registers can be monitored by the security office. This allows actual thieves to be confronted outside the store without disturbing legitimate customers (I refer to "false alarms", as the need for a paper record of purchases and confirmation by the clerk will disrupt the use of that cash register after its use by a thief).

Minnesota police have noticed that some shoplifters have been getting caught for many small thefts in different counties. Minnesota law allows many small losses during a six-month period to be added together, and if the total exceeds the minimum for a felony the thief may be charged with a felony. Police and major retailers are now sharing information on shoplifters so they can more severely prosecute the professional shoplifter. A database in a computer is being used to track the totals.

Anyone with access to the security system line from the cash registers can more conveniently gain information about any customer. Other than its invisibility, this is not much worse than the information disclosed to the clerks or the other persons waiting in line. However, if a store does not already use the purchase information for marketing purposes, the installed equipment can easily deliver information to a marketing system.

The thief database is more of a threat to thieves than to the general public, except of course in cases of mistaken identity.

Scot E. Wilcoxon, Data Progress, Minneapolis, MN +1 612-825-2607
sewilco@DataPg.MN.ORG {amdahl|hpda}!bungia!datapg!sewilco

(Counter-)corrective control systems

Jeffrey R Kell <JEFF@UTCVM.BITNET>
Wed, 23 Nov 88 11:23:40 EST

Last week, our operator informed me that our laser printer was indicating a low voltage condition. Indeed, the expected 240v was down to 214v, just below the 216v minimum allowed by the controller software. We contacted physical plant, who in turn discovered the building mains were also low. Next in line was the power board, who reluctantly investigated and after some deliberation and delay concluded that it was within their limits. This continued until we contacted the second shift supervisor at the power board and confirmed that the voltage was 10% below nominal. They tweaked the appropriate substation and voltage came back to normal.

On the following morning, the low 214v returned. Similar iterations of the previous day followed, and voltage again restored late that afternoon.

Next morning, as you might guess, 214v again, etc.

Eventually the power board's two shifts finally communicated. There was a bad (miscalibrated) sensor at some point showing a higher voltage than was really there. This was known to the second shift crew, who compensated accordingly (without correcting the sensor); but first shift was taking the reading verbatim.

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 85

Thursday 1 December 1988

Contents

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

Security Pacific Automated Teller Theft

Peter Neumann <neumann@csl.sri.com>
Wed, 30 Nov 1988 11:21:32 PST

Security Pacific National Bank acknowledged that nearly $350,000 was stolen on 11-13 November from about 300 customer accounts. A specially privileged "passkey" card may have been used from various LA-area ATMs to gain access to each of these accounts, without requiring the PIN number and without being subject to the daily limits on individual accounts. (One person reportedly had $1200 taken on a single day, in 4 installments) [Source: Los Angeles Times adaptation in S.F. Chronicle, 30 Nov 88, p. A6]

"Any system can be beaten," said a security official at another Los Angeles bank when told of the loss. [...] A security official at another Los Angeles bank, however, discounted the idea of a passkey. He did say that such a theft would almost certainly require inside knowledge. [From the original LA Times article by Douglas Frantz, Times Staff Writer, contributed by Stan Stahl (Stahl@DOCKMASTER.ARPA)]

[Superuser-type trapdoor mechanisms may be more useful for illegitimate purpose than for legitimate purposes. Having spent many years designing structured systems that were sufficiently flexible WITHOUT having such mechanisms, I wonder why systems with relatively omnipotent trapdoors

continue to be used in critical applications. The existence of such an ATM trapdoor seems highly unnecessary, and is clearly an invitation to misuse. Maintenance interfaces should be subjected to security and integrity controls, separation of duties, principle of least privilege, etc., just like everything else. PGN]

Corps of Software Engineers? (RISKS-7.84)

Dave Parnas <parnas@qucis.queensu.ca>
Wed, 30 Nov 88 23:15:02 EST

> "Flexibility is software's strong suit, allowing the military
> to make changes in how a weapon system functions, even after
> it is fielded... [discussion of gratuitous changes deleted]
> ...making changes in a hurry during a conflict is imperative
> if software is to help US forces prevail."
>
> [...] But where is the US corp of software engineers that can fix
> a key software module quickly so the next airstrike can account for
> an unexpected SAM threat? Do the armed services expect contractor
> personnel to volunteer for duty on the front lines? ..... "
> Henry Spencer at U of Toronto Zoology

Yes. I have seen battlefield trucks from Viet Nam whose walls were full of debugging notes. Contractor personnel were assigned to debug the programs during battle.

David L. Parnas, Queen's University, Kingston Ontario

Telecommunications, Data Entry and Worker Exploitation

Larry Hunter <hunter-larry@YALE.ARPA>
Thu, 1 Dec 88 16:29:36 EST

From "Optical Information Systems Update," Dec 1, 1988, p.8.

Digiport, a new telecommunications facility in Jamaica, will open up a new era for data entry operations. Two-way telecommunication eliminates one of the major problems of offshore data entry -- lengthly turnaround time. Previously, at least three to four days were required just for round trip flights. With image transmission, the data is quickly available for keying. In addition to fast turnaround, two-way transmission provides complete document control and security because the forms never leave the customers office. With this technology, the data entry function is electronically transferred to a low cost labor area with significant savings. For information, contact ... Offshore Information Services, Inc., 39 North Broadway, Tarrrytown, NJ 10591....

And, of course, with a significant loss to data entry personnel in high cost (like $6.00/hr) labor areas. Not to mention the savings (losses) in reduced

requirements for worker benefits and safety standards.

Larry

Milnet Isolation

the terminal of Geoff Goodfellow <Geoff@fernwood.mpk.ca.us>
30 Nov 1988 17:29-PST

PENTAGON SEVERS MILITARY COMPUTER FROM NETWORK JAMMED BY VIRUS
By JOHN MARKOFF, c.1988 N.Y. Times News Service

NEW YORK _ The Pentagon said on Wednesday that it had temporarily severed the connections between a nonclassifed military computer network and the nationwide academic research and corporate computer network that was jammed last month by a computer virus program.

Department of Defense officials said technical difficulties led to the move. But several computer security experts said they had been told by Pentagon officials that the decision to cut off the network was made after an unknown intruder illegally gained entry recently to several computers operated by the military and defense contractors.

Computer specialists said they thought that the Pentagon had broken the connections while they tried to eliminate a security flaw in the computers in the military network.

The Department of Defense apparently acted after a computer at the Mitre Corp., a Bedford, Mass., company with several military contracts, was illegally entered several times during the past month. Officials at several universities in the United States and Canada said their computers had been used by the intruder to reach the Mitre computer.

A spokeswoman for Mitre confirmed Wednesday that one of its computers had been entered, but said no classified or sensitive information had been handled by the computers involved. ``The problem was detected and fixed within hours with no adverse consequences,'' Marcia Cohen said.

The military computer network, known as Milnet, connects hundreds of computers run by the military and businesses around the country and is linked through seven gateways to another larger computer network, Arpanet. It was Arpanet that was jammed last month when Robert T. Morris, a Cornell University graduate student, introduced a rogue program that jammed computers on the network.

In a brief statement, a spokesman at the Defense Communication Agency said the ties between Milnet and Arpanet, known as mail bridges, were severed at 10 p.m. Monday and that the connections were expected to be restored by Thursday.

``The Defense Communications Agency is taking advantage of the loop back to determine what the effects of disabling the mail bridges are,'' the statement said. ``The Network Information Center is collecting user statements and forwarding them to the Milnet manager.''

Several computer security experts said they had been told that the network connection, which permits military and academic researchers to exchange information, had been cut in response to the intruder.

``We tried to find out what was wrong (Tuesday) night after one of our users complained that he could not send mail,'' said John Rochlis, assistant network manager at the Massachusetts Institute of Technology.

``Inititally we were given the run around, but eventually they unofficially confirmed to us that the shut-off was security related.''

Clifford Stoll, a computer security expert at Harvard University, posted an electronic announcement on Arpanet Wednesday that Milnet was apparently disconnected as a result of someone breaking into several computers.

Several university officials said the intruder had shielded his location by routing telephone calls from his computer through several networks.

A manager at the Mathematics Faculty Computer Facility at the University of Waterloo in Canada said officials there learned that one of their computers had been illegally entered after receiving a call from Mitre.

He said the attacker had reached the Waterloo computer from several computers, including machines located at MIT, Stanford, the University of Washington and the University of North Carolina. He said that the attacks began on Nov. 3 and that some calls calls had been routed from England.

A spokeswoman for the Defense Communications Agency said that she had no information about the break-in.

Stoll said the intruder used a well-known computer security flaw to illegally enter the Milnet computers. The flaws are similar to those used by Morris' rogue program.

It involves a utility program called ``file transfer protocol'' that is intended as a convenience to permit remote users to transfer data files and programs over the network. The flaw is found in computers that run the Unix operating system.

The decision to disconnect the military computers upset a number of computer users around the country. Academic computer security experts suggested that the military may have used the wrong tactic to attempt to stop the illegal use of its machines.

``There is a fair amount of grumbling going on,'' said Donald Alvarez, an MIT astrophysicist. ``People think that this is an unreasonable approach to be taking.''

He said that the shutting of the mail gateways did not cause the disastrous computer shutdown that was created when the rogue program last month stalled as many as 6,000 machines around the country.

[By the way, things still do not appear to be back to normal.
Too bad. That means MILNET hosts are not receiving RISKS, and
also that I will have more headaches than usual with BARFMAIL. PGN]

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 86

Saturday 3 December 1988

Contents

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

Mix-up Impedes Romance

Kevyn Collins-Thompson <kcollinsthom@lion.waterloo.edu>
Fri, 2 Dec 88 12:02:38 EST

One day, after I logged in to my CMS account here, I discovered that new mail was waiting for me in my reader. The lengthy message was prefaced by the heading:

> "From: Mailer@<machine>: Your message could not be sent ..etc"
> "Reason: Address unknown..."

Upon scanning this returned letter, I discovered that it had not been written by me at all, and that the intended recipient and sender were

thousands of miles away, apparently the unfortunate victims of a random mailer screw-up. The first sentence of that letter, though, I will always remember:

> "My dearest Janice:
> At last, we have a method of non-verbal communication which is completely private..."

California Lotto computer crash

Hoffman.ElSegundo@Xerox.COM <Rodney Hoffman>
2 Dec 88 07:47:47 PST (Friday)

From two stories by Dan Morain in the 'Los Angeles Times' on Tuesday, Nov. 29 and Thursday, Dec. 1:

> The California Lottery will fine GTECH Corp. $208,500 for a weekend computer crash that left two-thirds of the Lotto terminals in Southern California unable to accept wagers. All 4,375 terminals in Southern California stopped working for 14 minutes in the peak betting period Saturday night. Two-thirds of the terminals remained down for the rest of the night.
>
> A newly installed telecommunications program for the main Southern California lotto computer malfunctioned. The problem was exacerbated by a GTECH operator who subsequently installed the wrong back-up program. The new program was designed to improve system reliability. It has been removed for testing. "There's little doubt that the error was caused by GTECH software, compounded by GTECH operator error," said a senior vice president for the company.
>
> The state's contract with GTECH allows it to charge the company $4000 for each minute that the system is not working, and $1000 a minute when it is unacceptably slow. Lottery officials say that in the last year, the computer system has been inoperable or unacceptably slow for 779 minutes, or 0.2% of the time.

Telecommunications, Data Entry, ... - and "Security"

n c state univ <Henry Schaffer <hes@uncecs.edu<>
Fri, 2 Dec 88 15:39:08 est

Re: the quote from "Optical Information Systems Update," Dec 1, 1988, p.8.

> ... two-way transmission provides complete document control and security because the forms never leave the customer[']s office. ...

Of course, if one is concerned about the security of the *information*, that is a different matter.

Re: Toll Road information collection

Dave Nedde <daven@weathertop.prime.com>
Mon, 28 Nov 88 13:00:21 EST

>From: oster@dewey.soe.Berkeley.EDU (David Phillip Oster)
>Is it fair to also stamp the tickets with the time of issue, so if the
>distance traveled divided by the time elapsed is greater than the average
>speed limit the toll taker can hand you a speeding ticket at the same time?
>An appropriate computer would help the toll taker in this task.

Alas, as a Mass police officer pointed out in an interview, you have to catch someone *in the act* of speeding to get them for it. Probably something to do with that annoying bill of rights...

Manufacturers' responsibilities for security --

Keith Hanlan <keithh%tartarus%bnr-fos@sri-unix.UUCP>
Fri, 2 Dec 88 16:13:14 EST

Vendors should provide proper tools for security

In RISKS 7.84, Brandon S. Allbery (allbery@ncoast.UUCP) explains that "Vendors have some blame, but their [naive] customers and [ignorant] salespeople have even more." This thesis is based on his observation and his experience that a great many small-scale customers have no inclination to incur the overhead of a 'secure' system.

From this, and the context of the article as a whole, I infer further, that Mr. Allbery's feeling is that vendors are thus catering to a lowest common denominator and, perhaps in keeping with the spirit of unix, leaving the details and deficiencies to those with specific requirements. I agree that this is most likely what has happened even though it is not a publicly advertised tenet of any product developer.

However, I feel that the vendors' laxities cannot be excused in the least. In fact, as the professionals with an understanding of the implications of security, or lack thereof, it is incumbent on them to produce a secure product which is still easy to install, maintain, and use. Proper tools could reduce the confusion and inconvenience which drives so many customers to take short-cuts. It would also enhance their product in all market areas.

In the wake of the Internet Worm we have seen claims that UNIX is intrinisically an insecure system and that this fact casts a pall on UNIX's current rise in popularity. (I personally think the UNIX casts a pall on computing as a whole but that is another issue. :-)) However, I still maintain that proper maintenance tools will go a long way to producing secure computer networks.

I have used several varieties of UNIX and the vendor's are always very quick to advertise their value-added features and embellishments.

However, how often, when porting or re-writing an operating system, do vendors take the opportunity to fix glaring bugs and deficiencies? "Compatibility!" you cry? What bug cannot be made a option left to the user's discretion? ("-B switch for historical reasons.")

I hope this current wave of concern will encourage the vendors to re-think their development strategies. Bug fixes are not that difficult. It is time for the unix operating system developers to doff their hacker's capes and stop reveling in the vagarities of Unix.

Keith Hanlan, Bell-Northern Research

Computer Malpractice

"David J. Farber" <farber@dsl.cis.upenn.edu>
Fri, 2 Dec 88 22:03:08 EST

The network worm (sometimes called virus) affair raises issues that are very important to our field. Both the BITNET Board of Trustees and the CSNET Executive Committee have been struck by the fact that many public comments on the event have contained statements such as, "We learned from it," "We will make sure technically it will not happen again," or "He did us a favor by showing...," unaccompanied by expressions of ethical concern.

We have succeeded as a profession technically in creating facilities -- the BITNET, CSNET and other components of the national research network -- which are now critical to the conduct of science and engineering in our nation's academic, industrial, and government research laboratories. Further, this technology has spread within our nation's commercial research and development organizations and even into their manufacturing and marketing.

Just as medical malpractice can have a serious effect on an individual's health, one of the costs of our success is that we are now in a position where misuse of our national and private computer networks can have as serious an effect on the nation's economic, fense, and social health. Yet while almost every medical college has at least one course on medical ethics and insists on the observance of ethical guidelines during practice, computer scientists seem to avoid such non-scientific issues.

The worm "experiment" caused a major disruption in the research community. Among other points of attack, the worm exploited a trapdoor that had been distributed as a software "feature". Many hours of talent were wasted finding and curing the problems raised by this "game". Many additional hours were lost when researchers were unable to access supercomputers and mail systems due to system overload and network shutdown.

We condemn the perpetration of such "experiments", "games", or "features" by workers in our field, be they students, faculty, researchers or providers. We are especially worried about widespread tendencies to justify, ignore, or perpetuate such breaches. We must behave as do our fellow scientists who have organized around comparable issues to enforce strong ethical practices in the conduct of experiments.

We propose to join with the relevant professional societies and the national research networks to form a Joint Ethics Committee charged with examining existing statements of professional ethics and modifying them as necessary in order to create a strong statement of networking ethics and recommendations for appropriate enforcement procedures.

Interesting Sidebar on worm and liability

<<WERTZCJ@SNYBUFVA.BITNET> Charles J. Wertz, Buffalo State College>
Sat, 3 Dec 88 09:12 EDT

Here is an extract of an interesting comment sent to BUG-LAN@SUVM
by magill@ENIAC.SEAS.UPENN.EDU (William Magill at Univ of Pa.)
"..the reason that security policy procedures are important is an issue of LIABILITY."

"The recent Internet worm was a case where KNOWN security holes were exploited. While what was done 'wasn't nice', it was indefensible from a point of view of liability. Put another way, had data been compromised, the fact that known security holes were not 'plugged' would have rendered the University/Hospital defenseless in a liability case."

Unfortunate Use of Term "cracker" in RISKS-7.84

<tanner@ki4pv.UUCP>
Thu Dec 1 20:56:25 1988

[RISKS-7.84] referred to the common practice among the semi-literate of trusting to God that "crackers" will not invade or damage their new computer systems.

As a native of God's Own Country, I must object to this use of the term "cracker" to refer to computer vandals and burglars. I suspect that our neighbours to the north (also known as crackers) would also object.

Dr. T. Andrews, Systems, CompuData, Inc. DeLand

Re: "crackers" and "Crackers", " 'jackers", and "snackers"

Peter Neumann <neumann@csl.sri.com>
Sat, 3 Dec 1988 16:23:12 PST

With initial caps, "Cracker" (as used in Florida or Georgia) is a proper noun, as opposed to "cracker" (as in the sense of a malevolent hacker). But in Spoken English, the subtlety is certainly lost.

But we do have a problem. We desperately need a convenient term like

"cracker", because the nonpejorative primary meaning of "hacker" needs to be defended vigorously against misuse by the press and others. Perhaps we could try to use "jacker" (or " 'jacker", short for hijacker) as someone who breaks into computer systems and subverts them.

How about "snacker" for someone who is a nonmalicious but exploratory benevolent hacker? When Bob Morris (the elder) was visiting Berkeley from Bell Labs for the year (around 1967?), he might have been classified as a snacker: he seemed to nibble at the edges of the Berkeley time-sharing system more than anyone else. In fact, whenever he walked into the terminal pool room, others would log out -- because the system tended to crash more often when Bob was logged in. (He stumbled onto quite a bunch of hitherto undetected bugs.) [Joe Bftsplk at Berkeley?]

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 87

Monday 5 December 1988

Contents

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

Value for money?

Jerry Harper <jharper@euroies.UUCP>
Sat, 3 Dec 88 20:42:33 GMT

This is excerpted from THE IRISH TIMES of two weeks back:

" OFFICIALS `COMMITTED [$67m] TO INADEQUATE COMPUTERS' "

The Department of Health was accused yesterday of committing some [$67m] of State funds to the purchase of an inadequate computer system for the health service. Eleven million pounds will already have been spent on the project by the end of this year, the Secretary of the Department of Health, Mr Liam Flanagan, told the Dail [our parliament] Committee of Public Accounts.

...[the decision taken in 1982 to computerise government services... deleted]

...Auditor General,Mr Patrick McDonnell, expressed his disquiet at the lack of planning since that date, and at the fact that no costing was done until May 1985, by which time [$67m] was committed...
...[deleted piece about the authorship of a report]
...Mr Flanagan said [$670,000] had been spent on management consultancy. In his opinion, this was value for money, despite the fact that some of the hardware proved to be inadequate with high maintenance costs, and certain items had to be sold off at half-price to health boards. In particular, the committee heard that threee of the mini-computers which had cost approximately [$227,000] were sold back to the supplier for [$123,000]. Two of these were subsequently supplied to the Eastern Health Board at [$41,000] each.
...[deleted piece about the report being referred to the Minister]"
The system being referred to was put together by McDonnell-Douglas and "looked after" by the closely related McAuto. An enormous amount of pressure was placed on hospital administrators and senior consultants to accept the system. The pressure came from the company through the usual sales hype and several politicians attempting to bend individuals ears. A senior consultant I know in one of the prestigious test site hospitals commented that he was astounded at the inferiority of what was being offered. It became so bad at one stage that maintenance people were practically living in the hospital. I don't attribute culpability for the deficiencies of the system to any of the companies involved but at the very least they should have beta-tested the system more thoroughly. The management consultancy firm could do with a little of that also.

Corps of Software Engineers

Gary Chapman <chapman@csli.Stanford.EDU>
Mon, 5 Dec 88 09:01:54 PST

Not exactly a risk of computers, but definitely a risk to software engineers: during the early days of the war in Vietnam, there were some IBM programmers and system engineers living in-country and working on Army computers. One day things got pretty hot--a rocket attack, I believe--and the IBM personnel demanded to be evacuated. The Army refused, saying they were essential to the war effort, that without them the computers would not perform. The IBM manager threatened to go to superior authorities, so the Army commander then said that the nearby airbase was under attack and there were no flights available for evacuation. I never heard the resolution of this story, but it was clear these programmers got more than they bargained for.

For many years there was a "special" draft for doctors--physicians were almost guaranteed two years of military service, simply because they were doctors. Might we see something similar for computer professionals in the future?

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

---

DEC Enet and "denial of service" attacks

Willie Smith, LTN Components Eng. <w_smith%wookie.DEC@decwrl.dec.com>
5 Dec 88 10:50

Over the five-day Thanksgiving weekend, the crackers of New England successfully perpetrated a denial-of-service attack on Digital's internal network. They managed to do this without touching a keyboard. Someone in Corporate-level management decided that the following actions were to be taken by all system managers:

The first was to shut down all the routers. This prevented any network traffic at all from travelling between different areas and broke the network into independent LANs. Essentially turning off the WAN....

The second step was to disable all dialins at all sites. This prevented hackers from gaining access to the machines in the first place. This included all external packet network hosts as well as local modems.

The third step was to shut down all "unattended" machines for the duration. This additional step prevented hackers from getting to the machines at all, and greatly reduced the incidence of unauthorised use. :+}

Well, to give them credit, it worked just fine! It also caused a bit of havoc in automatic distribution of Internet and Usenet postings, and gave those of us who like to dial in to read our mail and internal BBSs the weekend off. In fact, it was so successful that there are rumblings that it may be repeated as needed. Most of our internal mailers time out after 3 days, and many are set to one day to conserve disk space. I've been told that the free access to the net that we have been taking for granted is going to tighten up considerably due to frequent intrusions.

Willie Smith w_smith@wookie.dec.com w_smith%wookie.dec.com@decwrl.dec.com
{Usenet!Backbone}!decwrl!wookie.dec.com!w_smith

Re: Nonsecure passwords/computer ethics (/dev/*mem and superuser)

Paul E. McKenney <mckenney@spam.istc.sri.com>
Tue, 22 Nov 88 13:54:00 PST

In RISKS-7.74, PGN says:

> [. . .] In UNIX,
> the /dev/mem vulnerability (a "feature" to some) can be used to capture passwords in unencrypted form. Even the Gould UTX/32S C2 version of Unix still has that vulnerability.

UNIX systems -can- be configured so that they do not have this vulnerability.
All memory devices (e.g., /dev/mem) devices should be protected as follows:

```
cr--r-----  1 root     sys       3,   0 Jan 10  1987 /dev/mem
```

i.e., so that only the super-user (root) or members of the special group ``sys'' (some systems use group ``kmem'', but the principle is the same)

are allowed to access kernel memory. This may be accomplished with
the following commands:
```
   chown root /dev/mem /dev/kmem ...
   chgrp sys /dev/mem /dev/kmem ...
   chmod 440 /dev/mem /dev/kmem ...
```
where the ``...'' is replaced by the pathnames of any system-specific
memory devices (e.g., /dev/vme* on Suns).

System programs that need access to kernel memory (e.g., ps) should have the
following protections:
```
   -rwxr-sr-x  1 bin      sys        47104 Jan 10  1987 /bin/ps*
```
i.e., the ``ps'' program should not be writeable to anyone except the
special user ``bin'', should be executable and readable to all, and should
set its group ID to ``sys'' upon execution (allowing it to read the /dev/mem
file). This prevents normal (read ``malicious'') access to the /dev/mem file,
while allowing authorized systems programs access to /dev/mem.
This may be accomplished with the following commands:
```
   chown bin /bin/ps ...
   chgrp sys /bin/ps ...
   chmod 4755 /bin/ps ...
```
where the ``...'' is replaced by the pathnames of all system programs
that need access to memory devices.

Note that the ptrace system call (which allows transparent debugging)
disables the setuid/setgid facility in the versions of UNIX that I am
familiar with. If your UNIX is less paranoid, you will also need to
disallow read access to system programs that access /dev/mem.

Thanx, Paul

Re: Nonsecure passwords/computer ethics (/dev/*mem and superuser)

Kendall Collett <kcollett@fang>
Fri, 18 Nov 88 09:30:55 -0600

> From: Peter G. Neumann <Neumann@KL.SRI.COM> (RISKS-7.74)
> Even the Gould UTX/32S C2 version of Unix still has that vulnerability. [...]

While the memory pseudo-devices (/dev/*mem) exist in Gould UTX/32S, access to
these devices is restricted in two ways (beyond the mode bits on the files):

1) All untrusted users in UTX/32S operate from within a
restricted environment (RE). An RE is a subtree of the file
system which, for the most part, looks like a complete UNIX
file system, with the exception that it does not contain
sensitive commands or files. When users log onto the system,
their root directory is set by the system to be the root
directory of the subtree forming the RE. Since an RE does
not contain the /dev/*mem files, from the user's perspective
the memory pseudo-devices do not even exist.

2) The memory pseudo-devices on UTX/32S are regarded by the

> system as ``privileged devices''. Regardless of the mode
> bits on the device special file, only superusers and can
> access privileged devices.

It is true a superuser on UTX/32S can access /dev/mem and read unencrypted passwords, but this does not give a superuser any capabilities that he or she didn't already have.

Kendall Collett
formerly:
Motorola Inc., Microcomputer Division Gould Inc., Computer Systems Division
Urbana Design Center Software Development Center
1101 E. University Avenue
Urbana, IL 61801

kcollett@urbana.mcd.mot.com
uunet!uiucdcs!mcdurb!kcollett

Disclaimer: In expressing the above opinion, I am in no way acting as a representative of either Gould, Inc. or Motorola, Inc.

Re: Nonsecure passwords/computer ethics (/dev/*mem and superuser)

Peter G. Neumann <Neumann@KL.SRI.COM>
Mon, 5 Dec 88 10:11:11 PST

Recalling the $350,000 ATM scam (RISKS-7.85), the mere existence of a superuser mechanism (no matter how well you think it may be protected) is dangerous. For example, the Ethernet and Arpanet are wide open and unencrypted, with passwords flowing around. The moral of the story is, to a first approximation, assume everything is wide open and don't rely on computers and networks to protect you. To a second approximation, you (and your system administrators, and your system vendors) can do much better to protect you. But don't count on it. PGN

"Hackers," "crackers," "snackers," and ethics (RISKS-7.86)

Frank Maginnis <maginnis@community-chest.mitre.org>
Mon, 05 Dec 88 11:04:12 -0500

Perhaps we should consider a less forgiving attitude towards traditional "hackers," or "snackers," as they are styled here. There are serious ethical concerns with an "experimenter" who uses uninformed, unknowing subjects in his experiments -- which is what, in effect, is being characterized as non-malicious and deserving of a non-pejorative term. Moreover, in more mature scientific fields, such as medicine, it is not left up to the experimenter to decide for himself what is ethically acceptable; he or she must convince review boards that include both peers and (one hopes) members of the affected public.

Some might consider the comparison with medical research ethics overdrawn. But consider: suppose a medical researcher were caught introducing some virus -- a real one -- into the environment. Suppose he thought the virus benign, but it

turned out that it made several thousand people sick, perhaps people who were in some particularly susceptible population (UNIX system administrators, say). Not too sick: maybe just enough that they lost a day or two of work, suffered discomfort, some degree of mental anguish . . .

The computer profession imposes a risk on the general public if it allows individual experimenters, however well intentioned, to conduct experiments, demonstrations of vulnerability, or whatever, on "subjects" who do not know they are a part of the experiment, and have not consented to being so. We shouldn't condone such activity, even when the affected community is small (e.g. subscribers to a university's time-sharing network), or when the impact turns out to be benign. We don't need a non-pejorative term for such activity; we need a highly pejorative attitude towards it.

Frank Maginnis, MITRE Corporation, McLean, VA
(Standard disclaimers apply)

Re: "Hackers," "crackers," "snackers," and ethics

Peter G. Neumann <Neumann@KL.SRI.COM>
Mon, 5 Dec 88 10:27:35 PST

I am afraid my point may have been misunderstood. Bob Morris (Sr.) was using the Berkeley time sharing system (which might have been called experimental at the time) as an ordinary unprivileged user. Systems in development are generally flaky. He just happened to fall into traps that had been unwittingly left by the builders, but was not trying to crash the system.

It seems rather obvious that such problems should be found early and fixed, BEFORE users come to depend (unwisely?) on computer systems. (Perhaps we need to add ``slacker'' to the hacker-alias terminology?)

By the way, a discussion that we may need to get into (when the Internet worm has died down) is the issue of whistle-blowing. We generally persecute whistle-blowers. It may be the "shoot-the-messenger" syndrome.

On the Internet worm problem and other similar situations, RISKS contributors seem to look on two positions as antithetical. In fact these positions are not incompatible

* Hacking can be dangerous (to the hacker and the hackees). (The Internet Worm initiator SCREWED UP BADLY.)

* Our favorite systems and network technologies are FUNDAMENTALLY FLAWED. We should not be surprised by malicious attacks by malevolent hackers in the future.

Neither of these statements negates the other.

[Sorry if RISKS is overly devoted to related problems lately. It is just going with the flow (of contributions). PGN]

Re: "Re: "Hackers," "crackers," "snackers," and ethics"

Frank Maginnis <maginnis%community-chest.mitre.org@gateway.mitre.org>
Mon, 05 Dec 88 16:26:09 -0500

[...] I misunderstood you to say that he was actually trying to crash the system, albeit by doing legal things (i.e. a "Black Team" sort of effort). Actually, I was not trying to criticize Morris Sr., so much as an attitude that seems to be widespread, if not endemic, in the profession. This attitude can be seen in defenses of Morris Jr., along the lines of: "Well, it's too bad the worm got out of control, but what he was trying to do was really benevolent," etc. etc. I also wanted to inject into the continuing discussion of computer ethics the idea that we should adopt something like the notion of "informed consent," as it is applied in medical research. The question of whether a university time-sharing system should be considered "experimental" with respect to this kind of hacking might be one that a university review committee could consider. They could look into whether the users understand that hacking is going on, in the interest of improving the system, and are willing to accept the risks involved. But the hacker shouldn't consider that he has the right to conduct an experiment just because _he_ considers it to be in everyone's best interests.

Incidentally, with respect to your original item, I'm afraid that trying to change the connotation of a word once it has gotten into general circulation is like trying to command the tide not to come in. Just ask 3M ("cellophane"), Xerox, mathematicians who study chaos theory, grammarians who rail against "hopefully," etc. "Hacker" and "virus" will undoubtedly appear very soon in standard English dictionaries with the general public's understanding of the terms, not the profession's -- "hacker" probably already has! We'll just have to adapt.

Ethics and caution (the worm)

Darrell Long <darrell@midgard.ucsc.edu>
Mon, 5 Dec 88 10:58:45 PST

I have seen several articles recently complaining about others that state they learned from the Internet worm and that the perpetrator actually did them a favor. The worm caused all of us to lose a lot of time, and so it was a serious breech of ethics. But I would like to remind everyone, that the real bad guys do not share our ethics, and thus are not bound by them. We should make it as difficult as possible (while preserving an environment conducive to research) for this to happen again.

The worm opened some eyes. Let's not close them again by saying "Gentlemen don't release worms."

Darrell Long, Computer and Information Sciences, University of California
Santa Cruz, CA 95064

"Hackers," "crackers," "snackers," and ethics (RISKS-7.86)

Alex Colvin <mac3n@babbage.acc.virginia.edu>
Mon Dec 5 14:21:58 1988

> But we do have a problem. We desperately need a convenient term like
> "cracker", because the nonpejorative primary meaning of "hacker" needs to be
> defended vigorously against misuse by the press and others. ...

In my youth (10 years ago) "hacker" WAS a pejorative term, implying a sort of dedicated misdirection. Those were the guys who spent all night writing login emulators and talk programs that they could eavesdrop. See Weizenbaum "Computer Power and Human Reason" for similar usage.

I forget what was the term of approval. "bit banger?"

Computer Risks Revisited

<John Markoff>
Sat, 3 Dec 88 09:12:40 PST

NETWORKS OF COMPUTERS AT RISK FROM INVADERS
By JOHN MARKOFF (c.1988 N.Y. Times News Service)

Basic security flaws similar to the ones that let intruders gain illegal entry to military computer networks in recent weeks are far more common than is generally believed, system designers and researchers say.

And there is widespread concern that computer networks used for everyday activities like making airline reservations and controlling the telephone system are highly vulnerable to attacks by invaders considerably less skilled than the graduate student whose rogue program jammed a nationwide computer network last month.

For example, the air traffic control system could be crippled if someone deliberately put wrong instructions into the network, effectively blinding controllers guiding airplanes.

The two recent episodes have involved military computers: one at the Mitre Corp., a company with Pentagon contracts, and the other into Arpanet, a Defense Department network with links to colleges. But illegal access to computer systems can compromise the privacy of millions of people.

In 1984, TRW Inc. acknowledged that a password providing access to 90 million credit histories in its files had been stolen and posted on a computerized bulletin board system. The company said the password may have been used for as long as a month.

This year an internal memorandum at Pacific Bell disclosed that sophisticated invaders had illegally gained access to telephone network switching equipment to enter private company computers and monitor telephone conversations.

Computer security flaws have also been exploited to destroy data. In March 1986 a computer burglar gained access by telephone to the office computer of Rep. Ed Zschau of California, destroyed files and caused the computer to break down. Four days later, staff workers for Rep. John McCain of Arizona, now a senator, told the police they had discovered that someone outside their

office had reached into McCain's computer and destroyed hundreds of letters and mailing addresses.

In Australia last year, a skilled saboteur attacked dozens of computers by destroying an underground communication switch. The attack cut off thousands of telephone lines and rendered dozens of computers, including those at the country's largest banks, useless for an entire day.

Experts say the vulnerability of commercial computers is often compounded by fundamental design flaws that are ignored until they are exposed in a glaring incident. ``Some vulnerabilities exist in every system,'' said Peter Neumann, a computer scientist at SRI International in Menlo Park, Calif. ``In the past, the vendors have not really wanted to recognize this.''

Design flaws are becoming increasingly important because of the rapidly changing nature of computer communications. Most computers were once isolated from one another. But in the last decade networks expanded dramatically, letting computers exchange information and making virtually all large commercial systems accessible from remote places. But computer designers seeking to shore up security flaws face a troubling paradox: by openly discussing the flaws, they potentially make vulnerabilities more known and thus open to sabotage.

Dr. Fred Cohen, a computer scientist at the University of Cincinnati, said most computer networks were dangerously vulnerable. ``The basic problem is that we haven't been doing networks long enough to know how to implement protection,'' Cohen said.

The recent rogue program was written by Robert Tappan Morris, a 23-year-old Cornell University graduate student in computer science, friends of his have said. The program appears to have been designed to copy itself harmlessly from computer to computer in a Department of Defense network, the Arpanet. Instead a design error caused it to replicate madly out of control, ultimately jamming more than 6,000 computers in this country's most serious computer virus attack.

For the computer industry, the Arpanet incident has revealed how security flaws have generally been ignored. Cohen said most networks, in effect, made computers vulnerable by placing entry passwords and other secret information inside every machine. In addition, most information passing through networks is not secretly coded. While such encryption would solve much of the vulnerability problem, it would be costly. It would also slow communication between computers and generally make networks much less flexible and convenient.

Encryption of data is the backbone of security in computers used by military and intelligence agencies. The Arpanet network, which links computers at colleges, corporate research centers and military bases, is not encrypted.

The lack of security for such information underscored the fact that until now there has been little concern about protecting data.

Most commercial systems give the people who run them broad power over all parts of the operation. If an illicit user obtains the privileges held by a system manager, all information in the system becomes accessible to tampering.

The federal government is pushing for a new class of military and intelligence computer in which all information would be divided so that access to one area did not easily grant access to others, even if security was breached.

The goal is to have these compartmentalized security systems in place by 1992.

On the other hand, one of the most powerful features of modern

computers is that they permit many users to share information easily; this is lost when security is added.

In 1985 the Defense Department designed standards for secure computer systems, embodied in the Orange Book, a volume that defines criteria for different levels of computer security. The National Computer Security Center, a division of the National Security Agency, is now charged with determining if government computer systems meet these standards.

But academic and private computer systems are not required to meet these standards, and there is no federal plan to urge them on the private sector. But computer manufacturers who want to sell their machines to the government for military or intelligence use must now design them to meet the Pentagon standards.

Security weaknesses can also be introduced inadvertently by changes in the complex programs that control computers, which was the way Morris's program entered computers in the Arpanet. These security weaknesses can also be secretly left in by programmers for their convenience.

One of the most difficult aspects of maintaining adequate computer security comes in updating programs that might be running at thousands of places around the world once flaws are found.

Even after corrective instructions are distributed, many computer sites often do not close the loopholes, because the right administrator did not receive the new instructions or realize their importance.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 88

Tuesday 6 December 1988

Contents

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

Summary of Software Uniformity Legislation issue

Conleth OConnell <cso@cis.ohio-state.edu>
Mon, 5 Dec 88 22:58:25 EST

I want to thank all of you who have expressed opinions on the Software Uniformity issue. I also want to forward the thanks of the organization, described below, for your opinions/concerns. After describing the organization, I give a brief summary of the opinions that were sent. To the best of my knowledge, the organization is meeting towards the end of January, so should you still want to send an opinion to me, I am setting a deadline of January 15, 1989, to insure forwarding. Once again THANKS!!

The organization that was requesting the information is "The National Conference of Commissioners on Uniform State Laws." The best known act that came out of this organization is the Uniform Commercial Code. It is made up of practicing lawyers, college law professors and deans, as well as some judges. The members donate their time to this organization although some states pay actual expenses, no member receives a salary for working on the organization. The organization has NO association with the Federal Government or with Congress. For those of you so inclined, the representatives from each state can be sought out via the State Bar or Secretary of State.

PROS

- Something needs to be done along the lines of truth in advertising of a particular product. For example, the packaging of some products with "lavish painted covers of the boxes". When in fact, the product has nothing to do with the artwork. This is not acceptable in other industries like videotapes, toys or plastic models.

- The industry has been lax with self-regulation, so something needs to be done.

- Some minimum standards are needed, but who monitors them, what are the reporting/registration requirements, what would be the penalties, but "Don't feed the lawyers."

CONS

- Most of the opinions were dubious of federal legislation even the opinions in the above section.

- A major concern is for the smaller companies/individuals.

- A bad product tends to get negative publicity anyway, thus there seems to be some quality control by the community, but the inexperienced/isolated user can get burned.

- Concern about price increase blamed on the regulation, which, in the end, hits the consumer and the small companies.

- "Control will only close off creativity."

- The Uniform Commercial Code has been used in the past.

- The feeling that the industry is "moving towards warranties, guarantees, and efforts for solid support" without legislation.

- Legislation may be obsolete by the new technologies.

- Similar feelings towards the "stifling" of public domain and free/shareware packages.

Thanks again and Happy Holidays!!
Conleth S. O'Connell, Department of Computer and Information Science,
The Ohio State University, 2036 Neil Ave., Columbus, OH USA 43210-1277

Exploiting workers

Dale Worley <worley@compass.UUCP>
Mon, 5 Dec 88 10:52:08 EST

> From: Larry Hunter <hunter-larry@YALE.ARPA>
>
> >From "Optical Information Systems Update," Dec 1, 1988, p.8.
>
> Digiport, a new telecommunications facility in Jamaica, will open up
> a new era for data entry operations.
>
> And, of course, with a significant loss to data entry personnel in high cost
> (like $6.00/hr) labor areas. Not to mention the savings (losses) in reduced
> requirements for worker benefits and safety standards.

Is this really a loss to the workers? The workers in the high-cost areas must be able to get $6/hr somewhere else (or else the data entry operations wouldn't have to pay so much). The workers in Jamaica clearly *aren't* able to get $6/hr somewhere else. It seems to me that the net change is to slightly reduce labor demand in high-wage areas (thus slightly reducing wages there) and to slightly increase labor demand in a low-wage area (thus slightly increasing wages there). It seems to me that this is not only "economically efficient" but also redistributes wealth from the rich to the poor. (Of course, an American data-entry worker isn't "rich" from our point of view, but *is* from the vantage point of the average Jamaican.)

If everybody in the world were able to bid on every job that they were capable of, wage inequities (from country to country) would be much smaller. This is what has happened in the automobile industry (modulo import restrictions), raising such formerly Third-World countries as South Korea into the ranks of industrialized nations.

Dale Worley, Compass, Inc. mit-eddie!think!compass!worley
Seen in a net discussion: "It took work to make tofu politically correct."

Re: Automated teller theft (Risks 7.85)

Dr Robert Frederking <ref@ztivax.siemens.com>
Tue, 6 Dec 88 14:15:19 -0100

I wouldn't be too sure that there really was a "passkey" card; that may have been a story cooked up to explain the loss to the public without revealing how vulnerable the system actually is. I don't know what technology is currently being used, but about 10 years ago a friend and I were looking at some used computer equipment we were thinking of buying, in someone's garage. After we

had chatted for a bit, and he apparently decided we were trustworthy, he told us that these computers were part of a banking machine system that he had bought, lock, stock, and barrel, and asked us if we would like to see the parts he wouldn't sell, for risk of being a party to a crime.

Among other things, there was a bank card reader that would display the account and *PIN number* of a bank card you ran through it. It could also *write* these cards. There was a set of sixteen thumbwheels inside the machine to set parameters to the encoding algorithm, which no one at the bank thought to shuffle, and so were still set to the bank's choice! He pointed out that once a set of positions was chosen, a bank would never change them again, as this would require recalling all the cards in circulation for recoding. It isn't clear to me that this could have been used in this case (unless the PIN number is algorithmically related to the account number, or the thieves had access to a list of PIN numbers), but this fellow could have caused a fair amount of trouble if he had been dishonest.

As for the daily limit, a friend of mine figured out once that you could easily exceed the daily limit. First ask for a balance. If the machine says it can't give you a balance at the moment, it means the line to the central database is down. You then withdraw the maximum daily amount. You do this on as many different machines as you can find. If the net is down, this is the total number of machines you can physically get to before the net comes back up.

"Robert Frederking" <unido!ztivax!ref@uunet.UU.NET>

Speeding detectors

Dave Horsfall <dave@stcns3.stc.oz.au>
Tue, 6 Dec 88 10:47:05 est

Just heard on the radio about how an Aussie inventor has come up with a box to detect speeders. Apparently, it ignores a short burst of speeding (e.g. overtaking) but logs it if it was sustained. When vehicle registration time comes around, the owner gets hit with a fine.

I missed the actual implementation details, such as how it knows what the current speed limit is (but bar code scanners were mentioned). The RISKS are obvious - you enter a 110 km/h zone, but the sensor doesn't see the new limit, and still thinks you are on 80 km/h etc.

In all, this appears to be yet another revenue-collecting device, shrouded in the guise of safety. We can well do without them.

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

[By the way, Dave accidentally reposted RISKS-7.65 to some of you, and wishes to extend his apologies. PGN]

Report of hardware "virus" on chips

Gary Chapman <chapman@csli.Stanford.EDU>
Mon, 5 Dec 88 15:59:16 PST

Advanced Military Computing, a defense industry newsletter, has reported that researchers at Nova University in Fort Lauderdale, Florida, have found a flaw in the Intel 8272A and NEC 765 floppy disk controllers that will allow incorrect data to be written to disks without alerting the user with an error message. The newsletter reports this flaw is a "virus," but there is very little technical information on the nature of the chip problem. The chips have been manufactured since 1978 and are estimated to be in millions of computers. Both NEC and Intel deny there is a problem, but an Intel memo dated May 2, 1988 admits an error in the Intel chip.

"The error condition has to happen in the last byte of the 512 bytes of a sector being transferred," said Nova University professor of computer science Phil Adams. The Intel memo, or letter, says that under this condition, "incorrect data is written to the disk and validated by the 8272A." The error condition is most likely to happen in networks and uploads to mainframes.

A report on the chip problem is available from Dean Edward Simco, of the Nova Computer Science Center, Nova University, Fort Lauderdale, FL 33314. The report is $5 and comes with a diskette containing a "risk assessment program," which allegedly reports on the "virus" in the subject machine.

[I assume no responsibility for the accuracy of this report, and this information is passed on without permission from Advanced Military Computing, and after no investigation of this other than reading the article in the newsletter.--GC]

-- Gary Chapman chapman@csli.stanford.edu
Executive Director, Computer Professionals for Social Responsibility

---

Re: Corps of Software Engineers?

Richard Rosenthal <richr@ai.etl.army.mil>
Tue, 6 Dec 88 12:36:54 EST

> "Flexibility is software's strong suit, allowing the military
> to make changes in how a weapon system functions, even after
> it is fielded...

Replacement chips are available for the microprocessors in cars allowing one to change the performance characteristics of the engine. Imagine the following conversation:

> Hey, Captain! Do you want one of these PROM's I burned last night?
> I changed the parameters for the F-16 thrust settings. Now I'll
> be able to do Mach 1.5 straight off the deck!

Vendor Liability, and "Plain Vanilla" configurations

"FIDLER::ESTELL" <estell%fidler.decnet@nwc.arpa>
5 Dec 88 12:51:00 PDT

GM *could* ship cars with "holes in the frame" for seatbelts, and then *highly recommend* that one order the seatbelts. They don't. The belts come, standard equipment, flat price; ditto the dashboard warning light and buzzer. Now, one *can* disconnect that annoying buzzer, or short out the connection under the seat to fool the buzzer. The cars are NOT tamper proof; but they are shipped with driver safety in mind.

By analogy, DEC could ship VMS with all the passwords "expiring" most ESPECIALLY those on "privileged" accounts [e.g., System, Operator], and then go into a "closed loop" that could be exited only after the "user" [system, or operator, in this case] selected and installed a *computer generated* password. ONLY then could the installation be completed; only then could the privileged accounts of "system managers" execute routines to allow users to generate their own passwords, default files to "public access" etc. etc. etc. ad insecurity.

I'm not picking on DEC; I happen to use -- and like -- VMS. I use that example because I can make it credibly. As most of you know, VMS is one of the few systems that has earned its "C2."

Bob

Talk on Computer Fraud

Mark Mandel <Mandel@BCO-MULTICS.HBI.HONEYWELL.COM>
Mon, 5 Dec 88 11:06 EST

Topic: "Computer Fraud: Motivation, Method and Opportunity"
Speaker: Tom Blake, Arthur Young, Boston,
Date: Wed 14 Dec 5:30 pm Anthony's Pier 4 Boston
Host: Mayflower Chapter, ASM (Association for Systems Management)
Register: Beth Furey (617) 367-3161 Admission/registration charge: $25.00

---

defining "hackers and crackers"

Gordon Meyer <TK0GRM1@NIU.BITNET>
Mon, 05 Dec 88 21:24 CST

I would argue that creating a new term to refer to the more... "illicit" users of computer system would do little to help solve the confusion. In my experience the "less malicious" use of the word HACKER is found almost entirely in professional computing circles. The media and general public know the term to mean "illegal, unauthorized and malicious computer use". (I just made that definition up...the quotes are used for emphasis not to indicate another source.)

If the computer science community continues to hold on to the term "hacker" they will only create more confusion and ambiguity in the future. While I

realize that the term may be nostalgic for some of you, english is not a static language and continuing to use an "outdated" definition of the term serves little purpose.

PS: Just to add a little more confusion to the issue, the term "cracker" is sometimes used to refer to those software pirates with the programming ability to remove copy protection. If folks insist on creating a new name for the "illicit" users out there..."crackers" is probably not the best choice. <grin>

Gordon R. Meyer, Dept of Sociology, Northern Illinois University.
GEnie: GRMEYER CIS: 72307,1502 Phone: (815) 753-0365

<[somewhere in netland]>
6 Dec 88 06:02:08 GMT

ames!pasteur!ucbvax!KL.SRI.COM!RISKS
Subject: RISKS DIGEST 7.87 [RISKS OF GREATER GARBLE]

I EXCERPTED A FEW GARBLED LINES FROM A RETURNED COPY OF RISKS-7.87.
[SIC] GLORIOUS TRANSIT MONDAY's ISSUE.

RIQKS-LIST: RISKS-FORUM Digest Molday 5 December 1988 Volume 7 8 Issue 87
FORUM ON RISJS TO THE PUBLIC IN COMPUTERS AN@ RELATED SYSTEMS
ACM Committee on Computers and Public Poli`y, Peter G. Neumann, moderator
DEC @net and "denial of service" att`cks (Willie Smith)
(P`ul E. McKenney, Kendall Collett, PGN)
(Fpank Maginnis, PGN, FM, Darrell @ong, Alex Colvin)
Computer Riqks Revisited (John Markoff)
taste, objective, aoherent, concise, and nonrepetitious. Diversity is welcome.
COLTRIBUTIONS to RISKS@CSL.SRI.COM(with relevant, substantive "Su`ject:" line
From: Jerry Harp`r <jharper@euroies.UUCP>
This is exaerpted from THE IRISH TIMES of pwo weeks back:
The Department mf Health was accused yesterday of committing some [$67m] of State funds to the purchase of an iladequate computer system for the health service. Eleven millimn pounds will already have been spent on the project Flanagan, told the Dail [our parliament] Committee of Public A`counts.
...[the decision taken in 1982 to computerise governmenp services... deleted]
...Auditor General,Mr Patrick McDonnell, expressed his disquiet at tha lack of planning since that date, and at the fact that no cost`ng was done until May 1985, by thich time [$67m] was committed.$.
...Lr Flanagan said [$670,000] had `een spent on management consult`ncy. In his opinion, this was talue for money, despite the fact that some of the hardware provdd to be inadequate with high maantenance costs, and certain itels had to be sold off at half-prhce to health boards. In particqlar, the committee heard that threee of the mini-computers whic` had cost approximately subsequently supplied to t`e Eastern Health Board at [$41,000] each.
...[deleted piece about the report being referred po the Minister]"
"loojed after" by the closely related McAuto. An enormous amount of pressure system. Thd pressure came from the company through the usual sales hype an` several politicians attempting to bend individuals ears. A selior consultant I

one stage that maintenan`e people were practically livind in the hospital. I don't attrhbute culpability for the deficiencies of the system to any of t`e
Not exactly a risk of computerp, but definitely a risk to softrare engineers: during the early days of the war in Vietnam, thepe were some IBM programmers war effort, that without thel the computers would not perform. The IBM manager threatened tn go to superior authorities, so the Army commander then said that the nearby airbase was under `ttack and there were no flights available for evacuation. I neper heard the resolution of this story, but it was clear these ppogrammers got more than they bapgained for.

[And then it is OK after that. The last time we ran such an item, it was a compression/decompression screw-up. Here it is just delted or garpled characters. I thought that there might have been an addded character, but then I noticed that "threee" is in the original. The time has come, the Mailrus said, or is this the legend of Tut? (See Path, above.) PGN]

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 89

Tuesday 6 December 1988

Contents

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

Computer Literacy #4

Ronni Rosenberg <ronni@wheaties.ai.mit.edu>
Tue, 6 Dec 88 15:12:11 EST

What are your reactions to a proposal for a different sort of "computer literacy" course, described below? (I am not saying that all schools should teach such a course.) Is it a good or bad idea? Why? Should the description be changed? If so, how? How do you compare this with what you know about existing computer-literacy courses? Who should develop such a curriculum? Who should pay for it? Please respond directly to me. Thanks.

* * * *

Compared to current computer-literacy classes, the proposed course would spend

much less time reviewing the mechanics of operating machines, the syntax of applications software or programming languages, and rote learning of lists, from computer components to uses. It would spend much more time considering the capabilities and limitations of computers, through discussions of the impacts of important computer applications. This might be a standalone course or a series of discussions interwoven into courses in, for instance, social studies or history.

One specific example of material that could contribute to meaningful education about computers is a multi-media presentation entitled "Reliability and Risk: Computers and Nuclear War," produced and distributed by CPSR. The presentation explains how current political and military trends decrease the time allowed for people to react to a crisis, thereby shifting critical decision-making responsibilities to computers. It attacks the myth of computer infallibility by describing different types of computer errors, their sources and consequences. It explores the growing reliance on computerized decision-making and how a computer error, especially in times of crisis, could trigger an accidental nuclear war. Lasting a half-hour, the program obviously cannot cover the topic in great depth. But it does present salient points about an important and complex area of computer use, greatly heightens people's awareness of problems that they are unlikely to learn about from magazine articles about computers, and stimulates exciting discussions and further thought. The presentation uses no computers, and the intended audience need no previous computer experience.

The proposed course might include discussions of

* SDI's computing requirements -- so students could consider the concept of software trusthworthiness and the potential for design errors in complex systems.
* The Vincennes episode -- so they could consider the difficulty of using a system outside the boundaries of its intended use.
* The FBI's National Crime Information Center (NCIC) -- so they could consider the relationship between civil liberties and computer technology.
* The National Test Bed, war games -- so they could consider the limits of computer simulations.
* Computerized monitoring techniques -- so they could consider impacts of computers on the workplace.
* How computer science is funded -- so they could consider which sorts of problems society views as important.
* Some of the myriad of RISKS stories -- so they could consider the risks of depending on computer systems.

And so on. Overall, the course would emphasize the importance of the social and political context in which a computer system is developed and used.

Privacy versus honesty/equality

Jerry Carlin <jmc@ptsfa.PacBell.COM>
1 Dec 88 20:45:26 GMT

The following is from an article: "In Sweden, the public can read prime minister's mail" by Eva Janzon, Associated Press.

In Sweden, government records have been open to the public since 1766. This includes the right to read the Prime Minister's mail (except for a few classified items). Not only that, but everyone's records are effectively public:

> "Knowing your neighbor's date of birth is enough to gain access to files at the National Taxation Board which lists income and tax from the previous year, church membership, marital status and current address.
>
> "If you take the number to the county police, you can find out about any unpaid bills. Other registers list education, state of health and membership in associations.
>
> "All this has been accepted as a price for keeping people honest in a society that strives for equality."

The article did state that some Swedes dislike this invasion of privacy.

Is the risk of inequality and dishonesty more important than the risk to privacy?

Jerry Carlin (415) 823-2441 {bellcore,sun,ames,pyramid}!pacbell!jmc

---

Computerized speeding tickets?

"Clifford Johnson" <GA.CJJ@Forsythe.Stanford.EDU>
Mon, 5 Dec 88 17:54:29 PST

> Alas, as a Mass police officer pointed out in an interview, you have to catch
> someone *in the act* of speeding to get them for it. Probably something to
> do with that annoying bill of rights...

Not so in every state, I believe. I recall a news story some 18 years ago in a desert state (Arizona?), in which a cop called a another cop at another town to look out for a certain car. The defense argued that there was no way to know to for sure that the speed limit was exceeded merely because the distance/time in total exceeded the speed limit. A university mathematician (measure theorist) testified as to the meaning of the Mean Value Theorem, and the speeding ticket was upheld by a presumably puzzled judge because no counter-expert could be found to dispute him.

Does anyone know whether the Mass. "rule" is simply local?

> [And then there is the tale of the San Francisco police using computer records interactively to tow up-scale vehicles (on the grounds that their owners are more likely to pay up to get their cars back when towed). Yesterday they towed a car belonging to an undercover agent. Referring to Ronni's item (particularly NCIC) in this issue, suppose that information was in the computer that that car belonged to an undercover agent. Then we have to assume that the agent was NOT ADEQUATELY under

cover, especially if any further identification was included. PGN]

Subways that "know" who's on board

Marc J Balcer <balcer@gypsy.siemens.com>
Tue, 6 Dec 88 09:38:49 EST

From the Philadelphia Inquirer, Saturday, December 3:

SEPTA TURNSTILES TAKE A HIGH-TECH SPIN
by Mark Bowden, Inquirer Staff Writer

[...] The new turnstiles still accept tokens, but they are also equipped with magnetic scanners that enable passengers to let themselves into the station just by sliding through their new, magnetically encoded weekly and monthly passes. The old turnstiles only accepted tokens. [...] Because each of the turnstiles is connected to a central computer, and each card is encoded with a serial number, use of the new turnstiles will help SEPTA compile far more detailed records of how people use the transit system.

"If someone gets on the Elevated in the Northeast, uses the Broad Street Subway at midday, and then commutes home at night on the Elevated, we will have an exact record of all those trips," said [Robert E.] Wooten, SEPTA assistant general manager for public affairs." It will provide our operations planning department with lots of detailed information about who gets on where, when, and how often.

Marc J. Balcer [balcer@gypsy.siemens.com] (609) 734-6531
Siemens Research Center, 755 College Road East, Princeton, NJ 08540

Automatic toll systems -- Dallas

<c60a-1bl@WEB.Berkeley.EDU>
Tue, 6 Dec 88 00:19:16 PST

Regarding an earlier discussion of automatic toll systems:

This evening (~11:45pm PST) on CNN, I caught the tail end of a report on an automated toll-collection system being tested in Dallas. The device consists of (and I quote) "chips and diodes and capacitors on a board", and is apparently queried at each toll station. During a brief statement, the president(?) of AMTECH, Inc. discussed plans for the use of this system in many cities and in the rail network.

Anyone have comments or more information?
(I wish I had seen the beginning of the report...)

Andrew R. MacBride c60a-1bl@widow.berkeley.edu (128.32.185.4)

"Hackers", "crackers", "snackers", and ethics (RISKS-7.86)

"Maj. Doug Hardie" <Hardie@DOCKMASTER.ARPA>
Tue, 6 Dec 88 09:42 EST

> Moreover, in more mature scientific fields, such as medicine, it
> is not left up to the experimenter to decide for himself what is
> ethically acceptable; he or she must convince review boards that
> include both peers and (one hopes) members of the affected public.

The cost of medical research is significant. It is not within the resources of your average high school student. The cost of hacking "computer research" is very low. I seriously doubt that any kind of review system could be set up that would be able to cope with the volume of this problem. Even if you could set it up, it would be a bureaucracy unto itself.

Also, I point out that the term hacker was in common use when I was in college (64-69) to refer to a person who did not have any real understanding of what they were doing, but just banged away with anything in a random pattern hoping that something would work. Calling an engineering student a hacker was the ultimate put down.

`hacker' is already a dictionary entry

Joe Morris (jcmorris@mitre.arpa) <jcmorris@mitre.arpa>
Tue, 06 Dec 88 11:38:21 EST

In RISKS-7.87, Frank Maginnis observes:
> "Hacker" and "virus" will undoubtedly
>appear very soon in standard English dictionaries with the general public's
>understanding of the terms, not the profession's -- "hacker" probably
>already has! We'll just have to adapt.

I can't speak for 'virus', but 'hacker' is already there. From the 1986 edition of _Webster's_New_World_Dictionary_ (Prentice-Hall) comes the following entry:

> hack.er n. 1. a person who hacks (see hack(1)) 2. an unskilled golfer, tennis player, etc. 3. a talented amateur user of computers, specif. one who attempts to gain unauthorized access to files in various systems

The dictionary doesn't have the verb _hack_ defined in a computer sense, but that may be waiting on the next edition.

Can anyone point to the first use of the term? I remember using it in 1962 (and have comments in programs to prove it) but it seemed to be well-used by then.

Re: "Hackers," "crackers," "snackers," and ethics

Douglas Jones <jones@herky.cs.uiowa.edu>

Tue, 6 Dec 88 13:51:24 CST

In P. G. Neumann's note of Mon, 5 Dec 88 10:27:35 PST, he points out that we have to do something about whistle-blowing, and then gets back to questions of hacking being dangerous, especially when we have flawed systems. These two statements bring to mind a sensible buisness practice of the early 1970's that I have not seen used recently.

Back in the summer of 1972, I worked for Com-Share Incorporated, one of two firms to commercialize the Berkeley Timesharing System. Back then, I had not yet heard the term "hacker", but we certainly knew that there were such people. Com-Share had two interesting policies with regard to such people:

1) All Com-Share employees were encouraged to use Com-Share facilities for personal use during off-hours, and the majority of personal use was assumed to be of a sort we would now call hacking.

2) Com-Share had a standing reward of $500 for anyone who could expose a flaw in their system security, and while I was there, they raised the reward to $1000.

In concert, these policies encouraged hacking, but they made it into a constructive activity. An occasionally cited aspect of the "hacker ethic" is that when hackers find something wrong with a system, they should report the problem. The problem is that reporting a problem might lead to its being fixed, which in turn, might deny future access to the hacker. A reward can overcome this negative aspect of reporting bugs.

When I worked on the PLATO system at Illinois in the mid '70s, the system administrators viewed the large community of PLATO hackers (mostly writing and playing games, but with occasional password security attacks of the kmem variety) as useful because they would exercise new system features long before "legitimate" users would find them, and because they provided a heavy system load before there was much of a legitimate user community. As the legitimate community grew and the excess capacity of the system diminished, game playing and other "hacking" activities were severely curtailed, but never eliminated.

In recent years, most computer crimes legislation I have seen has made almost anything resembling hacking into a crime, and many system administrators no-longer appear interested in the benefits that a carefully managed hacker community can provide. A hacker who finds a flaw in a system and reports it is viewed as being a criminal with a conscience instead of a benefit to society.

In a way, hackers who report flaws that they find in a system are like whistleblowers, and this recent legal and managerial trend is quite analogous to the "shoot-the-messenger" approach that is commonly applied to whistleblowers.

Re: /dev/*mem and superuser

Jeff Makey <Makey@LOGICON.ARPA>
6 Dec 1988 1258-PST (Tuesday)

In RISKS 7.87, Paul E. McKenney <mckenney@spam.istc.sri.com> described how to protect /dev/*mem on UNIX systems from uncontrolled read access. Unfortunately, he made a small mistake. /bin/ps and other programs that need access to /dev/mem should have their modes set to 2755. Use of mode 4755 (as Paul suggested) sets the setuid bit rather than the setgid bit. Since /dev/mem is owned by root and Paul also suggested changing the owner of /bin/ps to bin, there is probably no security problem in his fix, but ps won't work.

I have done this on my 4.2 BSD system with no apparent ill effects. In addition to /bin/ps, /usr/ucb/w needs this treatment.

Once again, we encounter a risk in (blindly) applying untested bugfixes. This comment, of course, applies to my own suggestions in the paragraphs above.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 90

Thursday 8 December 1988

Contents

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

"Glass cockpit" syndrome / Vincennes

Rodney Hoffman <Hoffman.ElSegundo@Xerox.com>
6 Dec 88 21:24:53 PST (Tuesday)

The 5 December 1988 'Los Angeles Times' reprints a lengthy 'Washington Post' story by Sally Squires with the headline and caption:

PERIL FOR PILOTS

> Psychologists call it the "glass cockpit" syndrome, a computer information overload in which the flood of technical information, faulty communication and outside stress lead to judgment errors.

Much of the article is drawn from testimony by American Psychological Assn. representatives before the House Armed Forces Committee, relating to the Vincennes shootdown in July of an Iranian commercial jetliner. The

witnesses said the incident "was just a symptom of a larger problem facing society." A few quotes from the article:

> Research is badly needed to understand just how much automation to introduce -- and when to introduce it -- in situations where the ultimate control and responsibility must rest with human operators, said Richard Pew of BBN....
>
> The growing use of high-tech devices in the cockpit or on ships can have two seemingly contradictory effects. One response is to lull crew members into a false sense of security. They "regard the computer's recommendation as more authoritative than is warranted," Pew said. "They tend to rely on the system and take a less active role in control." UTexas psychologist Robert Helmreich calls it "automation complacency."
>
> Another response is to fall victim to information overload and ignore the many bits of data pouring from myriad technical systems.... The stress of combat or poor weather or machine failure only serves to compound the errors that can be made. Yet "most military personnel feel impervious to stress," Helmreich said....
>
> But many stress effects can be overcome even in combat -- if people are conscious of their vulnerability.... Helmreich noted that when "multiple people verify information and decisions" there is less chance of error....
>
> "Errors of the sort made by Vincennes personnel can be anticipated, and procedures to reduce their likelihood or their gravity can be instituted," said UMichigan psychologist Richard Nisbett....
>
> [Background on the multiple emergencies aboard the Vincennes at the time of the shootdown.] "The anti-air warfare officer made no attempt to confirm the reports [from the crew] on his own," the commander-in-chief of the US Central Command reported. "Quick reference to the console directly in front of him would have immediately shown increasing, not decreasing, altitude [of the Iranian jet]." Instead, this "experienced and highly qualified officer, despite all of his training, relied on the judgment of one or two second-class petty officers, buttressed by his own preconceived perception of the threat, and made an erroneous assessment to his commanding officer."

VDTs and premature loss of ability to focus eyes

Rodney Hoffman <Hoffman.ElSegundo@Xerox.com>
6 Dec 88 21:00:21 PST (Tuesday)

The 5 December 1988 'Los Angeles Times' reprinted a story from the November 1988 issue of the UCBerkeley 'Wellness Letter' headlined PREMATURE LOSS OF ABILITY TO FOCUS EYES LINKED TO VDT USE.

The article reports on clinical findings by Dr. James Sheedy, chief of the VDT clinic at the UCBerkeley School of Optometry. Sheedy emphasized that

his evidence is preliminary and that his conclusions are based on people who had come to the clinic with eye problems -- not on a controlled study. These preliminary findings:

> Of 153 patients who averaged six hours a day at a VDT for four or more years, more than half had difficulty changing focus. Presbyopia, or loss of ability to focus with advancing age, accounted for half of these problems. The rest of the patients, though, were in their 20s and 30s and should have had good focusing mechanisms.

The article goes on to recommend appropriate eyeglasses, nonreflective screens, frequent breaks, etc.

NEW YORK TIMES reviews novel about computer sabotage

<jon@june.cs.washington.edu>
Wed, 07 Dec 88 09:10:40 PST

The Sunday, Dec. 4 issue of the NEW YORK TIMES BOOK REVIEW (their Christmas Books issue) prominently reviews a new novel, TRAPDOOR, by Bernard J. O'Keefe. The premise (from the review by Newgate Callender, NYT's crime fiction reviewer):

"A brilliant American woman of Lebanese descent has developed the computer code that controls the operation of all our nuclear devices. Turned down for the job she has sought, convinced male chauvinism is the reason, she is ripe to be conned by a Lebanese activist. At his suggestion she inserts a virus into the computer system that in a short time will render the entire American nuclear arsenal useless. ... The Lebanese President ... demands that Israel withdraw from the West Bank, or else he will tell the Russians that the United States will lie helpless for a week or so."

Callender's review begins with the lead sentence, "Nov 2, 1988, was the day computers in American went mad, thanks to the `virus' program inserted by the now-famous, fun-loving Robert T. Morris, Jr."

Some background on the author, also from the review:

"Bernard J. O'Keefe (is) chairman of the high-tech company EG&G and of an international task force on nuclear terrorism ... (and is) the author of a nonfiction book called NUCLEAR HOSTAGES. (O'Keefe says) "I wrote this parable to point out the complexity of modern technology and to demonstrate how one error, one misjudgment, or one act of sabotage could lead to actions that would annihilate civilization." "

Callender also says "...the execution is less brilliant than the idea. .. The book has the usual flashbacks, the usual stereotyped characters, the usual stiff dialogue."

Although the reviewer doesn't say so, the premise of this novel is quite similar to a 1985 French thriller, published in the U.S. as SOFTWAR. That novel was also based on the idea that a nation's arsenal could be completely

disabled from a single point of sabotage, although in SOFTWAR it was the Soviet Union on the receiving end. Popular reviewers of both books apparently find nothing implausible in the premise.

- Jonathan Jacky, University of Washington

---

meaning of "hack"

RAMontante <bobmon@iuvax.cs.indiana.edu>
Wed, 7 Dec 88 21:19:20 EST

I met the word "hack" at MIT in 1972, and I must admit that the current single-minded and increasingly pejorative usage bothers me. Let me quote from the Lexicon section of "How To Get Around MIT (1972 ed.)":

> Hack -- (1) A noun denoting a trick or prank. For example, welding a streetcar onto the tracks or getting elected UAP are fine hacks. (2) A verb meaning to goof off, talk randomly, or just hang around. (3) A verb meaning to apply oneself, work hard, try earnestly. Example: A computer hacker. Also connotes fanaticism. (4) Harrass somebody, whether in fun or maliciously.

Meaning (4) covers both the weather balloon planted in the Harvard-Yale football game some years ago, and the wishing well constructed in a friend's dorm room one holiday season.

One more quote from HoToGAMIT, under "THE OTHER EDUCATION":

> Metallurgy Shop
> For creative metallurgy or just hacking, 4-133 (the home of Tony Zona) is the place to be. you can learn welding, brazing, and soldering...

Hacker's Dictionary definition of Hacker

Russ Nelson <nelson@sun.soe.clarkson.edu>
Wed, 7 Dec 88 09:59:39 EST

Perhaps it's time to go to an authoritative source--the Hacker's Dictionary.

HACKER, noun.

1. A person who enjoys learning the details of computer systems and how to stretch their capabilities--as opposed to most users of computers, who prefer to learn only the minimum amount necessary.
2. One who programs enthusiastically, or who enjoys programming rather than just theorizing about programming.
3. A person capable of appreciating HACK VALUE.
4. A person who is good at programming quickly. (By the way, not everything a hacker produces is a hack.)
5. An expert on a particular program, or one who frequently does work using it or on it. Example: "A SAIL hacker." (This definition and the preceding ones are correlated, and people who

fit them congregate.)
6. An expert of any kind. One might be an astronomy hacker, for example.
7. A malicious or inquisitve meddler who tries to discover information by poking around. For example, a "password hacker" is one who tries, possibly by deceptive or illegal means, to discover other people's computer passwords. A "network hacker" is one who tries to learn about the computer network (possibly because he wants to improve it or possibly because he wants to interfere--one can tell the difference only by context and tone of voice).

---

hacker/cracker/snacker, and now: "slacker"

Douglas Monk <bro@rice.edu>
Wed, 7 Dec 88 15:45:10 CST

slacker : referring to a person who wrote sleazy or shoddy code but who should have known better, or was too lazy, or didn't think or care enough.

Doug Monk (bro@rice.edu)

Re: "cracker", "hacker."

Andrew Klossner <andrew%frip.gwd.tek.com@RELAY.CS.NET>
Tue, 6 Dec 88 15:11:17 PST

> "We desperately need a convenient term like "cracker", because the nonpejorative primary meaning of "hacker" needs to be defended vigorously against misuse by the press and others."

I disagree. The word "hacker" is now embedded in the American language to mean a computer attacker. No amount of energy spent railing against this new use will put an end to it, any more than we can make a plural noun again of "data."

Let's spend our vigorous efforts in areas that truly merit them.

-=- Andrew Klossner (uunet!tektronix!hammer!frip!andrew) [UUCP]
(andrew%frip.gwd.tek.com@relay.cs.net) [ARPA]

HACKERS CAN HELP YOUR SECURITY

SIANI@nssdca.GSFC.NASA.GOV <Kenneth Siani>
Thu, 8 Dec 88 15:24:14 EST

Much has been said recently about the evils of hackers and hacking.
I would like to say a few words in their defence.
Before entering the 'orthodox' computer security field, I myself

was a mysterious phantom of the night. :-) I am sure quite a number of persons in this field of computer security started out this way. Perhaps this fact gives me some insight on the subject of hackers.

I would like to clear up a few popular misconceptions about hackers. Hackers are not the people that destroy systems nor are they the people that penetrate systems to steal secret information or money. People that preform such acts are vandals and thieves, they are not true hackers. The only remote connection between such persons and hackers is the fact that both often do their work via modem and they both exploit weakness in computer security. Another thing that separates true hackers from the vandals that are mistakenly called hackers is motivation. Hackers are motivated by a great and intense quest for computer knowledge and perhaps the feeling of power that comes from it.
In addition, hackers have a true love of computers, and would never purposely damage any system. Destroyers of systems have no such love, and their motivations are quite different!

I am sure many of us have put a great deal of effort into making our systems as secure as possible. In our effort to make our systems secure, we have read the red book, the orange book, the MITRE reports and all the many other security related journals, books and reports.
We go to very expensive computer security seminars to hear wisdom from the experts and we try to implement all the safeguards the experts tell us about. Yet, the hackers still get in! Even the National Security Agency, the 'High Priests' of computer security, have had hackers running around their systems. Nobody seems to be immune to hackers!

Rather then focusing on the negative aspect of hacking and hackers, I would like to share with you a very positive experience with hackers that I was privileged to be a part of. During the summer of 87, I lead a group of real hackers on an assault of some of NASA's computer systems at the Goddard Space Flight Center in Greenbelt MD. One goal of this effort was to test the electronic venerability of selected computer systems at GSFC NASA. Another objective of this study was to raise the security consciousness of not only the key personnel of the selected target systems, but of all the users of the systems at GSFC.

This effort was known as "HACK ATTACK". A full report of all methods used and the success and failures of each were made. In addition, specific recommendations were made to improve the security of the penetrated systems. The official report is quite sensitive, but an unclassified yet very informative abstract of the report was presented at the AIAA/ASIS/IEEE Third Aerospace Computer Security Conference held in Orlando Florida Dec. 7th - 11th 1987.
You may wish to contact the American Institute of Aeronautics and Astronautics, 370 L'Enfant Promenade, SW, Washington, DC 20024-2518, for information about getting a copy of the report. The title is:
THE HACK ATTACK, INCREASING COMPUTER SYSTEM AWARENESS OF VULNERABILITY THREATS.

The Hack Attack was conducted in a very controlled manner, but the hackers were real and the results were a great surprize to all of us. Some of the hacker techniques employed were the Forward Hack, Reverse Hack, Default Account Hack, The Decoy and my personal favorite, Social Engineering. Some software bugs were exploited, as were some basic human weaknesses. The hackers ranged in experience, education and computer literacy from novice high school hackers to more experienced college level hackers. One thing shared by all of them and myself, was a great enthusiasm for the project. It truly was a game of wits, the hackers against the systems and their operators.
Some systems were penetrated while others were not. In the end there were no losers, only winners. The security weakness of some systems were exposed while the strengths of others were confirmed.

As a direct result of the Hack Attack some software has been modified and some policy has been changed. But the greatest change of all has been in the user community. The security consciousness of the users has greatly increased, and that was of course our primary goal. Perhaps your systems and users could benefit from such an experience. You would be surprized to find out just how many hackers would be willing to help you plug the holes in your system. You would be equally surprized how much more seriously your users would consider the issue of computer security after they have been exposed to a Hack Attack.

The Hack Attack has made a lasting impression on people.
It has been over a year since the Hack Attack, but to this very day, people cover up their terminal screens or log off their computers when I enter the room. :-)

DISCLAIMER: The views expressed here are my own and not that of my employer, NASA, the NSA, or any other person or government agency.

Kenneth Siani
Sr. Security Specialist
Internet address: { SIANI@NSSDCA.GSFC.NASA.GOV }

Hacking as a profession... Why not?

Don Mac Phee <BIW137@URIACC.BITNET>
Thu, 08 Dec 88 09:59:40 EST

I have been involved in mainframe computing for a number of years on systems ranging from an NCR mainframe (I've blissfully forgotten the type! :-)) through to a VAX 8600. And in my experience as a user, I've found that a hacker can be one of the greatest assets to a system. No administrator is omnipotent and sometimes they can make serious mistakes in the installation of a certain package, or pay negligible attention to loopholes in the operating system that

can lead to increased downtime or even worse... virus attacks that paralyze the system. But the question I pose to the RISKS reader is this:

Why don't the manufacturers hire 'hackers' to debug their operating systems? I'm not speaking of the countless consulting firms that do security work, or the people who designed the system. Instead, I speak specifically of the 'hacker' as a bright energetic person who sees the system from a different viewpoint from that of the administrator, or the designer. Someone who, when given a set of manuals about the design of the system and the operation, can 'break in' legitimately and show the flaws.

Maybe I'm naive, but isn't the best way to design a mousetrap, is to build it, then send the mice through?

-Don Mac Phee (BIW137@URIACC.BITNET)

Unquestioning belief in expert testimony

Matt Bishop <bishop@bear.Dartmouth.EDU>
Wed, 7 Dec 88 09:00:56 EST

In RISKS 7.89, Clifford Johnson tells of a speeder who was convicted because of testimony of a university mathematician involving the Mean Value Theorem. One of the risks of being involved with science and technology is that often we deal with things that the public does not completely understand, and so has to "take our word for". This can have quite drastic consequences.

Haber-Runyon's book "General Statistics" has a graphic example of this (see p. 156-157). An elderly woman was mugged in California, and a witness saw a "blonde girl with a ponytail run from the alley and jump into a yellow car driven by a bearded Negro." Eventually, a couple were arrested and tried for the crime; the evidence against them was that the woman "was white, blonde, and wore a ponytail while her Negro husband owned a yellow car and had a beard." Both were convicted, because the prosecutor got an expert witness from the math department of a nearby college to testify that the probability of a set of events occuring is the product of the probability of each of the events actually occurring; and using "conservative estimates" (such as the chances of a car's being yellow is 1 in 10, the chances of a couple in a car being interracial ia 1 in 1,000, etc.), he concluded the odds of any other couple sharing the characteristics of the defendents is 1 in 12,000,000. That was enough for the jury.

Fortunately, the California Supreme Court disagreed. Aside from the illegality of "trial by mathematics", the math expert didn't go far enough -- assuming everything he (or she) said was true, one Justice pointed out that there was a 41% chance that at least one other couple in the area will also share those characteristics! (He attached a 4 page appendix to the opinion demonstrating this to his own, and five concurring justices', satisfaction.)

Such are the dangers of encouraging blind trust in experts ...

Matt Bishop

PS: The woman was released earlier and broke parole when she "lit out for parts unknown." The man was in jail at the time of the Supreme Court's opinion; "he could be tried again, but the odds are against it."

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 91

Sunday 11 December 1988

Contents

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

More on Proper British Programs

<leveson@electron.LCS.MIT.EDU>
Fri, 09 Dec 88 13:00:37 -0500

You probably all know about the MoD draft standard in Great Britain requiring formal verification of safety-critical software. Well, here is another one. I was asked to consult on the safety of a microwave landing system, and they have just sent me a copy of a draft attachment to an international standard for MLS systems by the ICAO (international organization overseeing such aircraft systems). This may no longer be a draft -- there is no date on it and the company implied that they had to follow it. As you can see from the following, there is an "out," but the sophistication of the standard

is a surprise to me (most American software standards are abysmal). Since the ICAO must certify these systems before they are used, the standard has teeth and could be enforced quite strictly (unlikely, but ...). The following are some interesting excerpts:

> "... [Software] must be developed systematically in such a way that its behavior, under all possible conditions, can be established by logical reasoning (to a level of formality appropriate to the application).
>
> "... The programming should be performed in such a way that it is easily possible to establish the correspondence between the programme and its design and to verify its correctness with respect to its specification by logical reasoning (possibly supported by software tools).
>
> "... The interface of every software module with its enclosing environment should be explicitly stated in a preamble within its code, as well as in the design documentation. Where possible, a formal specification (e.g., in terms of pre- and post- conditions) should be given.
>
> "... Consistency of the code and its comments with the specification and the design documents should be checked, as formally and precisely as possible, as each module is developed. Formal verification (i.e., proofs of consistency between formal specifications of software modules and their code) should be performed where possible. Otherwise, manual code inspections or structured walk-throughs are essential. A software safety analysis should be performed as part of the design and development using at least one technique such as FMECA, fault tree analysis, or cause and consequence analysis..."

Re: Vendor Liability, and "Plain Vanilla" configurations (RISKS-7.88)

"Jay Elinsky" <ELINSKY%YKTVMX.BITNET@CUNYVM.CUNY.EDU>
Tue, 6 Dec 88 17:05:38 EST

Maybe GM and the other manufacturers *would* sell cars without seat belts and warning buzzers, if there wasn't a *law* requiring them. So if we accept this as a valid analogy (I'm not saying it is or isn't), then the conclusion is that we need a law requiring computers to have adequate security.

Jay Elinsky, IBM T.J. Watson Research Center, Yorktown Heights, NY
[Affiliation for identification only]

Manufacturers' Responsibilities for Security (RISKS-7.86)

Lynn R Grant <Grant@DOCKMASTER.ARPA>
Sun, 4 Dec 88 16:46 EST

Having been in the security software business for several years, I must take some exception to Keith Hanlan's comments on manufacturer's responsibilities for security. While I truly believe that some vendors use the excuses he mentioned for not making their products secure, there is some merit to them.

Security is not free. Those of us in this business do the best we can to make secure systems easy to use (at least the good ones among us do), but a wide open system is usually easier to use. Security involves a tradeoff: it what it costs you less than what you might lose without it. The customer may decide it isn't worth the cost. He may be wrong, but it's still his decision.

As for bugs, bugs should be fixed. But design flaws that influence security are trickier. For some reason, customers tend to find these flaws, and set up their production systems so they depend upon them. Thus, when you fix them, suddenly your customer's shops don't run anymore, and they get very irate. If your competitors do not fix the problem in their software, your customers see this as a feature, and it puts you at a competitive disadvantage. I can see how some vendors might knuckle under to this pressure, figuring that fighting for security ideals is of no use if all the customers flee for some less secure system and cause the company to fold up.

Let me reiterate that this is not a wholesale defense of those who ignore security in the name of ease of use (which may really be ease of implementation). I just want to point out the pressures that exist in the competitive arena of commercial software.

Lynn R. Grant, Technical Consultant, Computer Associates International, Inc.
Disclaimer: These opinions are my own, and may or may not reflect those of my employer.

[One man's feature is another man's future. But one person's feature can also be someone else's destruction. I am reminded of the multiple index register instructions in the IBM 7090 that stopped working in the 7094 because they were `only features' and were not officially supported. Anyone who lives by unsupported features may die the same way. PGN]

Hacker enters U.S. lab's computers

George Wood <wood@emmy.ma.UTEXAS.EDU>
Sat, 10 Dec 88 20:33:00 CST

Austin-American Statesman, Saturday, December 10, 1988, P. A29

Hacker enters U.S. lab's computers
By Thomas H. Maugh II, Los Angeles Times Service

A computer hacker has entered computers at the government's Lawrence Livermore Laboratory in the San Francisco Bay area eight times since last Saturday, but has not caused any damage and has not been able to enter computers that contain classified information, Livermore officials said Friday.

Nuclear weapons and the Star Wars defense system are designed at livermore, but information about those projects is kept in supercomputers that are physically and electronically separate from other computers at the laboratory.

The hacker, whose identitiy remains unknown, entered the

non-classified computer system at Livermore through INTERNET, a nationwide computer network that was shut down at the beginning of November by a computer virus. Chuck Cole, Livermore's chief of security, said the two incidents apparently are unrelated.

The hacker entered the computers through an operating system and then through a conventional telephone line, He gave himself "super-user" status, providing access to virtually all functions of the non-classified computer systems.

Officials quickly limited the super-user access, although they left some computers vulnerable to entry in the hope of catching the intruder.

"There has been no maliciousness so far," Cole said. "He could have destroyed data, but he didn't. he just looks through data files, operating records, and password files....It semms to be someone doing a joy-riding thing."

Computer Virus Eradication Act of 1988

Mon, 5 Dec 88 16:43:12 EST

[EXCERPT from VIRUS-L Digest V1 #33]

VIRUS-L Digest Monday, 5 Dec 1988 Volume 1 : Issue 33

Date: Mon, 5 Dec 88 11:11:06 EST
From: Don Alvarez <boomer@space.mit.edu>
Subject: Computer Virus Eradication Act of 1988

I just received a copy of HR-5061, a new bill being introduced in the House by Wally Herger (R-CA) and Robert Carr (D-Mich.). The text of the bill is included below (see disclaimer).

It sounds to me like there are some subscribers to VIRUS-L who's background is more criminal law than computer science, perhaps some of you could help the rest of us out with a little commentary. Would this bill be helpful to you? Do you think you would be able to get a conviction with it? Do you think you would be able to recover your damages with it (and how would you go about defining those damages if you were to use the law)?

If people are interested in sending their comments to the authors, I include the name and address of the legislative aide who has been working on this bill. If people would like to e-mail their comments, you can send them to me and I will mail them to him in a packet (be sure to include your name and normal postal mail adress, as congress isn't on the net).

Don Alvarez, boomer@SPACE.MIT.EDU

- ------Start of Bill

100th Congress 2D Session H.R. 5061

To amend title 18, United States Code, to provide penalties for persons interfering with the operations of computers through the use of programs containing hidden commands that can cause harm, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES July 14, 1988
Mr. Herger (for himself and Mr. Carr) introduced the following bill; which was referred to the Committee on the Judiciary

A BILL
To ammend title 18, United States Code, to provide penalties for persons interfering with the operations of computers through the use of programs containing hidden commands that can cause harm, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,
SECTION 1. SHORT TITLE.
This Act may be cited as the "Computer Virus Eradication Act of 1988".

- -------Page 2

SECTION 2. TITLE 18 AMENDMENT.
(a) IN GENERAL.- Chapter 65 (relating to malicious mischief) of title 18, United States Code, is amended by adding at the end the following:
"S 1368. Disseminating computer viruses and other harmful computer programs
"(a) Whoever knowingly-
"(1) inserts into a program for a computer information or commands, knowing or having reason to believe that such information or commands will cause loss to users of a computer on which such program is run or to those who rely on information processed on such computer; and
"(2) provides such a program to others in circumstances in which those others do not know of the insertion or its effects;
or attempts to do so, shall if any such conduct affects interstate or foreign commerce, be fined under this title or imprisoned not more than 10 years, or both.
"(b) Whoever suffers loss by reason of a violation of subsection (a) may, in a civil action against the violator, obtain appropriate relief. In a civil action under this section, the court may award to the prevailing party a reasonable attorney's fee and other litigation expenses.".

- --------Page 3

(b) CLERICAL AMENDMENT.- The table of sections at the begining of chapter 65 of title 18, United States Code, is amended by adding at the end the following:
"1368. Disseminating computer viruses and other harmful computer programs.".

- --------End of Bill

>>>>NOTE: The above text was typed in by hand from a printed copy of HR5061
>>>> received from Mr. Herger's office. I have no experience with
>>>> legal documents of this sort, and may have made typographical
>>>> errors which could affect the nature of the bill. Neither
>>>> I nor my employer (MIT Center for Space Research) make any claims
>>>> as to the accuracy of the text. For an official copy of the
>>>> bill, please contact:
>>>>
>>>> Mr. Doug Riggs
>>>> 1108 Longworth Bldg
>>>> Washington D.C. 20515

They did it: Speed-Thru Tollbooths

Robert Steven Glickstein <bobg+@andrew.cmu.edu>
Tue, 6 Dec 88 17:13:43 -0500 (EST)

A news report last night on the Headline News Channel reported the experimental installation of a new kind of tollbooth in Dallas, TX (I think?), and one or two other places. Instead of tossing money into a hopper, you just drive on through -- while a low-frequency, low-power radio signal polls an electronic "tag" taped to your windshield, which (hopefully) squawks a valid code back at it. (I was sort of amused to learn from the newscaster that this "tag" is made from "printed circuits, capacitors and diodes.") Reportedly, toll plazas in New York City and about a dozen other places will soon be outfitted with the new technology.

The problems with this system from a RISKS perspective are numerous and evident. Perhaps the most troubling is that the system works on an accounting principle. Your "tag" uniquely identifies itself to the transmitter in the tollbooth, and your passage is recorded. Presumably you then get a monthly bill from the highway people. The problem here, of course, is that when you drive through a tollbooth, Big Brother knows exactly where you are.

> *Excerpts from ext.in.risks: 18-Nov-88 Smart Roads (RISKS 7.81) Robert*
> *Brooks@sde.hp.com (1040)*
> Much concern has been expressed about the Big Brother potential of such
> systems. But this is by no means an essential hazard. The transponders,
> barcode tags, or whatever could be purchased anonymously, and authorization
> to cross various toll points n times purchased in advance, like postage
> stamps.

This would be fine, except that if the tags are completely indentity-free, then stolen tags become especially problematic -- the thief is in no danger of the tag becoming disabled, and the victim pays the thief's way through n tollbooth passages, where n could be quite large (and quite expensive, especially in New York, where tolls currently go as high as $3 for passenger cars). The temptation to thieves to break into cars so equipped would therefore be very great. In the current system, the tag is a non-descript black box secured above the registration/inspection stickers by Velcro strips. Even if a car owner were to hide the tag in the glove compartment when not in use, the Velcro

strips, permanently adhered to the windshield, are a dead giveaway.

The RISKS of theft are great even in the case of identifiable tags. The non-descriptness of these black boxes makes it easy for a thief to replace a stolen tag with a functionless dummy, so that it could be some time before the victim even realizes the unit had been stolen, by which time the thief could have run up quite a bill for the victim.

The greatest RISK posed by these units is that the subjects in the current experiment seem to unanimously love the idea. Just breeze through a toll-plaza -- great! It never occurs to the average technology-ignorant, computer-phobic user that there may be some serious security/privacy problems here. I think some sort of high-publicity demonstration of the flaws in this system are called for as soon as possible.

Bob Glickstein, Information Technology Center, Carnegie Mellon University, Pittsburgh, PA

[Dave Nedde: Re: Toll Road information collection]

Brint Cooper <abc@BRL.MIL>
Sat, 3 Dec 88 22:42:07 EST

Dave Nedde quotes David Oster:

<>From: oster@dewey.soe.Berkeley.EDU (David Phillip Oster)
<>Is it fair to also stamp the tickets with the time of issue, so if the
<>distance traveled divided by the time elapsed is greater than the average
<>speed limit the toll taker can hand you a speeding ticket at the same time?
<>An appropriate computer would help the toll taker in this task.

Then he adds:

>Alas, as a Mass police officer pointed out in an interview, you have to catch
>someone *in the act* of speeding to get them for it. Probably something to do
>with that annoying bill of rights...

I seriously doubt that the Mass. police officer is absolutely correct. After all, a favorite FBI strategy in catching professional hoodlums was to prosecute, successfully on income tax evasion. The evidence often was nothing more than a cash flow analysis: showing that someone spent more money in one year than he reported as income! Convictions were upheld, no?

Risk of computers? Sure; think how often sucn analyses are possible using computers: proving Medicaid fraud, failure to repay student loans, catching scofflaws who replace a revoked driver's licence in one state with a "good" one in another, etc.

Perhaps we should call this "benefits of computers?"
_Brint

Re: Toll Road information collection

Scott E. Preece <preece@xenurus.gould.com>
Mon, 5 Dec 88 09:48:28 CST

From: Dave Nedde <daven@weathertop.prime.com>
> Alas, as a Mass police officer pointed out in an interview, you have to
> catch someone *in the act* of speeding to get them for it. Probably
> something to do with that annoying bill of rights...

I suspect it would be trivial to modify the law if it in fact prohibits such an application now. The state has very broad discretion in controlling the use of public roads and the privileges and responsibilities of those who hold state licenses (they could make it a license requirement to report illegal traffic behavior and then fine all licensed drivers in a car known to have been speeding, if they chose to make the statutes work that way). I don't see any way the Bill of Rights is even remotely involved.

scott preece, motorola urbana design center uucp: uunet!uiucuxc!mcdurb!preece

---

Re: Toll Road information collection

<sullivan@fine.Princeton.EDU>
Sun, 4 Dec 88 14:13:39 EST

There was discussion of this in another newsgroup not too long ago. Someone pointed out that exiting the toll road with average speed greater than the speed limit does not prove you were driving over the speed limit, since you might have switcherd drivers. Maybe this defense would indeed hold up--I no lawyer--but I see no reason not to pass a new law to make exiting with too little elapsed time a new crime. The owner of a car can be held responsible for parking tickets even if someone else parked the car, so I see no reason that whoever drives through the exit booth can't be held responsible for the average speed.

John Sullivan

---

re: Subways that "know" who's on board

<Hibbert.pa@Xerox.COM>
Wed, 7 Dec 88 11:01:16 PST

Regarding the item about the philadelphia subway system's capability to track monthly pass-holders' movement:

I'm not particularly worried about this as an invasion of privacy, as long as purchasers don't have to identify themselves when buying their passes. It sounds to me as if the data they could collect doesn't contain any identification of individuals. It doesn't seem problematic for the transit commision to be able to gather statistics on individual traveller's routes, as long as there's no ability to tie the information to who the traveller is.

I confess that I don't see a usefull way to correlate information on different trips by the same individual. The most usefull information would be just what the starting and stopping points were. Without this tracking ability, they presumably can't tell what the distribution of trip lengths is, and there are probably ways to make use of that information.

Oh, I guess there might be a privacy problem if there is real-time feedback from the tracking system. For instance, if some police officer decides that lots of short trips throughout the day (as an example) is characteristic of some type of criminal of interest, it would be a problem if there were a way to find out real-time that someone fitting that description were right now passing through a particular turnstile.

Other than that possible hole, this seems like an example of a way to gather data that starts out as a description only of average or sample behavior. As I said, all this is wrong if users identify themselves when they buy their passes.

Chris

[Well, many people pay by check or credit card, and that information would of course have to be recorded, for bookkeeping reasons... PGN]

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 92

Monday 12 December 1988

Contents

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

Glass cockpits (Rodney Hoffman, RISKS-7.90)

Randall Davis <davis@wheaties.ai.mit.edu>
Sun, 11 Dec 88 16:23:32 EST

The article [Peril for Pilots] raises two interesting issues:

The larger issue is, what kinds of and how much remote sensing to use, what kinds of and how much automation to introduce in any situation. Note, though, that the problem of information overload and believing sensors (including your own eyes) has been with us for quite some time and exists /independent of/ automation in general and computers in particular. Both of those can easily ADD to the problem, but that's different from being the SOURCE of it.

Second, it is another example of the remarkably unsuccessful attempt to cast technology as the primary heavy in the Vincennes incident. When it first happened we saw a remarkable flood of messages to Risks speculating about the role of advanced automation in general and computers in particular as central to this disaster. When the report came out indicating that the system had supplied accurate information, the silence was deafening.

And now this (continuing from the same msg above):

> "The anti-air warfare officer made no attempt to confirm the reports [...] Instead, this "experienced and highly qualified officer [...] relied on the judgment of one or two second-class petty officers, buttressed by his own preconceived perception of the threat, and made an erroneous assessment to his commanding officer."

In other words, if only the AA Officer had <>paid attention to the system and believed it instead of or along with his ``one or two ... officers,''<< the tragedy would have been avoided.

Can automation and reliance on remote sensing be overdone? Of course. Is this an example of it, or an example of the opposite?

The point is not that technology is blameless, nor that this particular technology is faultless, nor that the sole issue is the effectiveness of the technology (political, ethical, military and other considerations all play a role in this).

The point is twofold:
first, within almost any reasonable definition, the system worked to supply accurate and useful information in a form available in a ``quick reference''; every report that comes out continues to make that clear.

second, there is, with only a few exceptions, clearly a strong desire in the Risks community to believe otherwise. Perhaps that's worth a few minutes reflection.

"Proper British Programs" (Nancy Leveson, RISKS-7.91)

Steve Philipson <steve@aurora.arc.nasa.gov>
Mon, 12 Dec 88 13:15:22 PST

>the ICAO must certify these systems before they are used, the standard has
>teeth and could be enforced quite strictly (unlikely, but ...). The following
>are some interesting excerpts:

> "... [Software] must be developed systematically in such a way that its
> behavior, under all possible conditions, can be established by logical
> reasoning (to a level of formality appropriate to the application).

It's my opinion that strict enforcement of the above requirement simply makes the developer liable for errors, but doesn't do much for actually

improving software reliability. It is unlikely that "all possible conditions" can be forseen, let alone provided for. The problem becomes bigger as the complexity of the system increases, to the point where exhaustive analysis of a system could take centuries to perform.

The requirement is essentially that systems be perfect. That goal has proven elusive (unattainable?) in all areas of human endeavor. Extensive formalism and verification should be required of critical systems, but requirements for perfect function are inane. A better approach would be to require independent performance monitoring and evaluation as part of the complete system. This is the approach we often take with non-computer based systems. It seems reasonable to make it part of our imbeded computer systems as well.

Toll Road information collection (John Sullivan, RISKS-7.91)

Steve Philipson <steve@aurora.arc.nasa.gov>
Mon, 12 Dec 88 13:15:22 PST

John Sullivan (sullivan@fine.Princeton.EDU) writes about fines for speeding based on computed speed from toll both timing:

> ... I'm no
>lawyer--but I see no reason not to pass a new law to make exiting with too
>little elapsed time a new crime. The owner of a car can be held responsible
>for parking tickets even if someone else parked the car, so I see no reason
>that whoever drives through the exit booth can't be held responsible for the
>average speed.

A parking violation does not go on a person's driving record. It does not matter who was cited as long as the bill is paid. So, if you lend your car to a friend who then get's a parking ticket, you can collect from him with no negative impact on your record. However, a speeding ticket does end up on a specific person's record, and thus can result in the suspension of that person's driving priveleges, and can have a significant impact on his/her insurance rates, etc. This makes it quite important to assign the ticket to the driver and not just the vehicle. This scheme does not address this concern, hence it is unreasonable.

Steve Philipson

Big Bother and Computer Risks

<dlm@cuuxb.att.com>

In reference to RISKS DIGEST 7.91, Robert Steven Glickstein <bobg+@andrew.cmu.edu> and others have been discussing Toolbooths and other risks of automated monitoring.

This subject has been extensively treated by Science Fiction writers, especially Mack Reynolds who postualed the Coporate State with a cashless society. All transactions were done with a single money card.

One story especially instructive involved a "criminal". He tried to rob a person and it was pointed out that the card was useless without the owner as personal identfication [e.g. retinal prints, etc.] were necessary to use the card. Our protagonist grabs the person, etc.

The police give chase and they are tracking the crook by observing the use of the card, and where it is used. Later they watch him use the Mass-Transit system and can track him to the gate and car.

The end of the story concludes that the "crook" is a cracker to test how easy it was to break the system and how long it would take for police to catch such a person.

Interesting points were that the tracking mechanism was built into the computer systems and could be activated on a widespread basis by a simple command from a computer. Our risk is that such capabilities could be designed into any new cashless machine either as a conscious feature or as a debug switch for testing.

I suspect that the case of life imitating art is close at hand and readers of the risks list ought to go back and check out some early Science Fiction as well as the latest Computer stories including the so-called cyber-punk movement.

=Dennis L. Mumaugh
Lisle, IL ...!{att,lll-crg}!cuuxb!dlm OR cuuxb!dlm@arpa.att.com

---

Information available for a price

<keller@ficc.UUCP>
Wed Dec 7 20:29:48 1988

I received a postcard in the paper mail from a company called Credit Checker and Nationwide SS#- Locate. Apparently anyone can -

- o Take a lot of risk out of doing business.
- o Check the credit of anyone, anywhere in the United States
- o Pull Automobile Drivers License information from 49 states
- o Trace people by their Social Security Number

By "Using ANY computer with a modem!"

To subscribe to this unique 24-hour on-line network call 1-800-255-6643.

Hmmm, I wonder if my neighbor with the new 928 : can really afford it
and how many traffic tickets does he have....

Curtis Keller

[Also noted on 12 Dec 88 by Bruce O'Neel <XRBEO@SCFVM.GSFC.NASA.GOV>]

Re: Computer Virus Eradication Act of 1988

Jonathan Sweedler <cjosta@taux01.UUCP>
12 Dec 88 07:42:38 GMT

From what I have read of the laws and bills dealing with computer viruses and computer trespassers, it seems that someone can only be prosecuted if they "cause harm" to a computer. Even the new Computer Virus Eradication Act of 1988 doesn't seem to apply to a person who enters a computer without authorization just to browse through directories. Even part two of the below quote from the act may be circumvented by simply announcing that you have entered the computer! It seems that Robert Morris Jr. would not have done anything illegal (even under these new bills) if his virus had worked as it was designed to work: to propagate quietly from machine to machine.

>7 "(a) Whoever knowingly-
>8 "(1) inserts into a program for a computer infor-
>9 mation or commands, knowing or having reason to be-
>10 lieve that such information or commands will cause
>11 loss to users of a computer on which such program is
>12 run or to those who rely on information processed on
>13 such computer; and
>14 "(2) provides such a program to others in circum-
>15 stances in which those others do not know of the inser-
>16 tion or its effects;

In other words, can I break into any computer I want to and look at whatever files I want to, as long as I announce I'm there and don't cause any harm? Why do these laws center on causing harm to computers and not just illegal/unauthorized entry?

Jonathan Sweedler === National Semiconductor Israel
Domain: cjosta@taux01.nsc.com

Computer Virus Eradication Act of 1988 (RISKS-7.91 from VIRUS-L)

Vince Manis <manis@grads.cs.ubc.ca>
Mon, 12 Dec 88 12:22:54 PST

>From: Don Alvarez <boomer@space.mit.edu>
>Subject: Computer Virus Eradication Act of 1988
>1 SECTION 2. TITLE 18 AMENDMENT.
>2 (a) IN GENERAL.- Chapter 65 (relating to malicious
>3 mischief) of title 18, United States Code, is amended by
>4 adding at the end the following:
>5 "S 1368. Disseminating computer viruses and other harm-
>6 ful computer programs
>7 "(a) Whoever knowingly-
>8 "(1) inserts into a program for a computer infor-
>9 mation or commands, knowing or having reason to be-

>10 lieve that such information or commands will cause
>11 loss to users of a computer on which such program is
>12 run or to those who rely on information processed on
>13 such computer; and
>14 "(2) provides such a program to others in circum-
>15 stances in which those others do not know of the inser-
>16 tion or its effects;
>17 or attempts to do so, shall if any such conduct affects
>18 interstate or foreign commerce, be fined under this title or
>19 imprisoned not more than 10 years, or both.

The idea sounds great to me. However, the wording has problems. I'm not a lawyer, but the text above appears to make it illegal to provide a delete file routine in an operating system; it also makes the GNU Emacs 'dissociated-press' function illegal.

What seems to be missing here is a proper definition of the terms 'virus' and 'worm'. Presumably, the problems with such programs are that: (a) they install themselves into computer systems surreptitiously, (b) they operate without the user asking them to do so, and (c) [viruses only] they damage user data. I don't think the above wording addresses these issues. There's also a question of intentionality: if a system includes a `Grim Reaper', which deletes all files not referenced within a certain period of time, and a user does not know about the G.R., are the implementors of the system, or the operations staff on that machine, responsible for the disappearance of files?

I consider it a RISK when legislators introduce bills on technological matters which may not really address the issue at hand. I remember Rep. Jack Brooks writing letters to Sigplan Notices about 20 years ago on why PL/I was a poorer language than Fortran and Cobol, for example. It is our job as technical people to advise legislators on such issues.

Of course, as a Canadian, why should I care...? :-)

Re: Vendor Liability and "Plain Vanilla" configurations

Andy Goldstein <goldstein%star.DEC@src.dec.com>
12 Dec 88 14:02

> From: "FIDLER::ESTELL" <estell%fidler.decnet@nwc.arpa>
> [...] By analogy, DEC could ship VMS with all the passwords "expiring" most
> ESPECIALLY those on "privileged" accounts [e.g., System, Operator], and then
> go into a "closed loop" that could be exited only after the "user" [system,
> or operator, in this case] selected and installed a *computer generated*
> password. ONLY then could the installation be completed ....

We've been doing that for a couple of years. All the standard passwords are set up pre-expired, and the installation prompts for new passwords on all the standard accounts (and rejects the standard values). The only thing we don't do is to generate the passwords; the password generator was considered too controversial. (The French really hate it because the letter frequency

is all wrong.) The biggest problem is that once you've installed a system, there are ways of cloning the system disk that circumvent the standard installation procedure. I feel it's still the most effective thing we've ever done for system security.

There are some other things that aren't as tight as we would like them in the out-of-the-box system; we're working on those. Thanx for your kind words; we keep trying.

- Andy Goldstein VMS Development

Re: "Hackers", "crackers", "snackers", and ethics

Andy Goldstein <goldstein%star.DEC@src.dec.com>
12 Dec 88 11:48

Douglas Jones points out some experiences with benign hacking in the 1970's, in which the efforts of friendly hackers helped improve the overall system. He expresses regret at the current attitude of treating all hackers as criminals.

I have had productive working relationships with hackers in the past, much to be benefit of my company's products, and I continue to maintain some of these relationships. However, this only works in some environments. Constructive hacking makes sense in universities and some development environments, where the hackers belong to the organization that operates the computer systems, giving them a certain level of trustworthiness. In addition, the data in such systems is not terribly valuable, and the occasional disruptions in service are a nuisance and no more.

With the majority of hacking nowadays, things are quite different. Many of the computer systems involved are crucial to a business's operation; some are critical to human life. The potential (and in some cases the actuality) is there for major losses from disruption of service and theft. The hackers are unknown outsiders in whom a serious organization can place no trust whatsoever. Today's hackers do not report what they find. Rather, they steal an organization's data and services. They leave trap doors for themselves so they can re-enter the system after it has been ostensibly secured. They are, simply put, electronic joyriders and vandals.

I am all in favor of constructive hacking, but it should be confined to safe places. Those who enter systems used for sensitive purposes should be prosecuted for the tresspass they have committed. [Easier said than done, of course, which is one of our biggest problems.]

Andy Goldstein, VMS Development

Hackers

Shatter <unido!altger!Shatter@uunet.UU.NET>
11 Dec 88 19:24:12 MEZ (Sun)

Well it is nice to at last see a responcible and inteligent attitude to hackers in risks (thnx Kenny), But i feel that it is time that an active hacker had some form of input into the current debate.

Before I get down to my arguements about hackers and hacking perhaps I should say a few words about myself and why I feel qualified to make my views known.[I expect I will get flamed alot after this]

Some of you may have already heard of me via articles in the WALL STREET JOURNAL, NEW YORK DAILY NEWS etc but for those of you who don't read or have access to copies of these newspapers I am a hacker of over 10 years activity who is based near Nottingham, England My speciality are the various packet switched networks around the world such as PSS,Telepac,Transpac etc with various forays into UN*X,NOS/VE VMS,VM/SP CMS (HPO) etc.[by the way I apologise for any spelling mistakes but my spelling is very bad as I am dyslecxic]

I feel that as a hacker with so much activity and expirience I am qualified to make the following points on behalf of the whole hacking community.

Hackers are not the vandals and common criminals you all think we are in fact most of the "TRUE" hackers around have a genuine respect and love for all forms of computers and the data that they contain and we are as a community very responcible and dedicated to the whole idea of IT but we also have a strong dislike to the abuse of IT that is perpitrated by various governments and organisations either directly or indirectly. There is of course a small minority of so called hackers who do cause trouble and crash systems or steal money etc but these people on the whole are dealt with by other hackers in away that most of you could not even think of and most never repeat their "crimes" again.

In risks recently you have all been very busy discussing what names to use for hackers and you all seem to be mssing the point. The term "HACKER" is still one to be very proud of and I am sure that in your younger days you were all called hackers and were very proud of the fact that someone felt that you had a great technical expertise that warrented the use of the term, But you all suffer from the standard problem that nearly all people involved within IT have and that is of non communication. You never pass on the information that you pickup and learn to others within IT [American Government organisations and Educational Institutes are among the greatest offenders] and this allows the hacking community [who do communicate] to be at least one step ahead of the system administrators when it comes to finding security problems and finding the cause and fix for the problem. A case in point is the recent arpanet worm and the FTP bug both these problems have been known for many months if not years but when talking to various system administrators recently not one of them had been informed about them and this left their systems wideopen even though they had done all they could to secure them with the information they had. [An interesting piece of information is that hackers in england knew about Morris's worm at least 12 hours before it became public knowledge and although England was not able to be infected due to the hardware in use we were able to inform the relevent people and patrol internet to janet gateways to look for any occurance of the worm and therefore we performed a valuble service to the computing community in England -- although we did not get any thanks or acknowledgement for this service.] [but i am straying] Hackers should be nurtured and helped to perform wot they consider a hobby [you may do a

crossword as an intelectual challenge -- I study computers and learn about how things interact together to function correctly (or incorrectly as the case may be)] and the use of a group of hackers in a "HACK ATTACK" ((c) Kenny 1988) can perform a valuable service and find problems that most of you could not even start to think of or would even have the inclination to look for.

So please don't treat us like lepers and paupers find yourself a "TAME" hacker and show him the respect he deserves and he will perform a valuble service for you and above all COMMUNICATE with each other don't keep information to yourselves if you have found it the chances are that so has someone else and horror apon horror it may be a HACKER

Bst Rgrds
Shatter

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 93

Tuesday 13 December 1988

Contents

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

Overrides of train controls in Japan

Jeff Schriebman <jeff@jusoft.jusoft.junet>
Tue, 13 Dec 88 09:04:24+0900

[@ucbvax.Berkeley.EDU,@unisoft:jeff@jusoft.UUCP]

Drivers Often Override ATS on Chuo-Sobu Line
Asahi Evening News, Thursday December 8, 1988

Tokyo, Japan -- Police investigating the Dec. 5 rear-end collision at Higashi-Nakano Station on the East Japan Railway's Chuo Line, which killed two [the driver and a passenger] and injured 102, have found that the train drivers override the ATS (automatic train stop) system over 10 times during

the run between Chiba and Mitaka stations.

This is because the heavy train schedules result in trains becoming close-packed on the tracks. Police also found that the drivers in many cases do not apply the hand brakes after overriding the ATS, as they are required to do, because applying the brakes would delay the trains further.

This practice of overriding the ATS and not applying the hand brakes is believed to be in the background of the Dec. 5 rear-end collision.

The investigations up to Wednesday showed that the brakes and ATS on the train that ran into the stopped train were in good working order.

JR East penalizes train drivers for being late more than 30 seconds when calculating pay hikes and bonuses. Drivers say JR East is stricter on this point than the old Japanese National Railways (JNR). The catchword is, "Don't be late!".

The train that ran into the stopped train was about four minutes behind schedule and JR people say that driver Teruki Hirano could have been trying to make up for lost time.

The union claims that the tight schedules produced the accident, but JR East points out that similar schedules have been used for more than 20 years. During the peak commuting hour in the morning, there are trains every two and a half minutes, but at the time of the accident, the interval was one every three and a half minutes.

This was the third accident on the down line between Okubo and Higashi-Nakano stations, and all three were rear-end collisions. They all occurred between 9 and 10 a.m. after the morning rush hour. Most passengers get off at Shinjuku Station, and drivers tend to relax because they have only a little more to go to Nakano Station or Mitaka Station [the end of their run].

No improvements were made in signal and safety facilities after the second accident in 1980. Some experts point out that there should be more signals installed at shorter intervals because of the sharp curve in front of the station and the short distance between the end of the curve and the station.

Re: Vincennes and over-reliance on automation

<RILEY@csvax.src.honeywell.com>
Tue, 13 Dec 88 15:16 CST

In RISKS 7.92, Randall Davis writes:

> Can automation and reliance on remote sensing be overdone? Of course.
> Is this an example of it, or an example of the opposite? [...] ...within
> almost any reasonable definition, the system worked to supply accurate
> and useful information in a form available in a "quick reference"; every
> report that comes out continues to make that clear.

And earlier in the same submission, "When the report came out that the system had supplied accurate information, the silence [among RISKS contributors] was deafening."

As I understand the final Pentagon-issued report on the Vincennes incident, the initial classification of the aircraft's identity and altitude vector were indeed in error. The October 15 Science News summarizes the findings thus: "The computerized surveillance system on the Vincennes first misread the plane's altitude and identified it as an F-14 fighter jet, but then corrected itself. The Navy report concludes crewmen responsible for evaluating surveillance did not closely analyze the initial computer mistake. Furthermore, the skipper paid more attention to their increasingly heated reports of an emergency than to new displays generated by the computer."

That being the case, one could make a case for this being an example of over-reliance on automation. The crew involved believed the initial system identification and altitude reading and did not double check them, nor did they change their evaluation when given new, conflicting information. However, when faced with an over-the-horizon threat, the crew has no choice but to rely on remote sensing and automated target identification, so over-reliance is hardly an option.

I think this incident was primarily the result of an interaction between automation and crew that system developers did not predict, and in fact have no way of anticipating without extremely extensive scenario generation and analysis. The crew was "primed" to accept the initial misidentification because a fire-fight with Iranian gunboats twenty minutes prior to the aircraft encounter had raised their expectation of attack and, in effect, lowered their target detection "threshold" to the point where the original misidentification was easily accepted.

As automation becomes more complex, and as decision-making becomes more automated, I think we'll see more of these types of incident. System developers need to realize that complex automation can produce subtle and unintended consequences, due to the interactions between automation and crew or between automated systems, and that these consequences can lead to major errors. I believe the major outcome of the Vincennes incident should not be to assign blame to either automation or humans, but rather to recognize that new analytic approaches should be developed to uncover potential problems before such systems are fielded.

-Victor Riley, Honeywell Systems and Research Center
(all usual disclamers apply)

Fake ATMs

Rick Adams <rick@uunet.UU.NET>
13 Dec 88 03:47:20 GMT

From Communications Week International, 21 Nov 88

One night last year, Italian banking clients using the ''bancomat,'' an electronic teller, were pleased to discover that their bank branch had added an extra terminal. Delighted to be spared waiting time, the clients inserted their cards into the machine. The bancomat presented the usual menu and requested the client's personal identification numbers. The machine, however, withheld the client's cards, informing them that the cards were invalid and that they should request information during banking hours. It was only when the clients returned to the bank the following day, ready to complain, that they learned that they had been victims of a new kind of fraud. What had appeared to be a bancomat was, in fact, a personal computer, placed on the bank wall by an independent operator. The thief/entrepeneur used the cards and identification numbers to clean out their accounts.

This anecdote, revealed recently during a conference of banking security experts, indicates the kind of problems faced by value-added services operators in a country that has serious organizational difficulties.

> [This is the old system-spoof problem. Authentication is a two-way street. The system needs some sort of authentication that the user identity is authentic. But the user also needs some sort of authentication that the system identity is authentic. PGN]

`Trapdoor' -- War by Computer Virus

Rodney Hoffman <Hoffman.ElSegundo@Xerox.com>
12 Dec 88 17:51:52 PST (Monday)

In the 11 Dec 88 'Los Angeles Times Book Review' Times Book Editor Jack Miles reviews a new novel, "Trapdoor" by Bernard J. O'Keefe (Houghton Mifflin). The headline for the review is WAR BY COMPUTER VIRUS. It quotes from the epilogue to the novel, in which the author calls it a "parable to point out the complexity of modern technology and to demonstrate how one error, one misjudgment, or one act of sabotage could lead to actions that would annihilate civilization."

I have not read the book, but according to the review, an inside saboteur plants a delayed-action "virus" (the review calls it one, although the description doesn't really sound like one) in a Pentagon computer which messes with the public-key encryption codes required to fire US missiles equipped with permissive action links. "The result: America no longer knows the code necessary to launch its own weapons. The nation is defenseless." (In the epilogue, the author points out that it can't quite happen that way.) Much more transpires.

The author, O'Keefe, earlier wrote the non-fiction "Nuclear Hostages," worked with Fermi and Oppenheimer on the Manhattan Project, and heads EG&G, the company which the publisher says has "conducted all nuclear weapons tests for the US government for the last 40 years and is the operating contractor for the Kennedy Space Center."

The reviewer says, "there remains a lean and gripping parable hiding inside an only slightly overweight thriller. For all its novelistic faults, I

can't imagine a timelier read or a better Christmas gift for anyone serious about computers or math.... If the computers that control our nuclear weapons can be disabled, what about the computer that control our nuclear power plants? What about the computers that control our vote-counting and our stock transactions?..."

Re: "Hackers", "crackers", "snackers", and ethics

Douglas Jones <jones@herky.cs.uiowa.edu>
Tue, 13 Dec 88 09:05:08 CST

In Andy Goldstein's contribution of 12 Dec 88, he says, in reaction to my previous comments:

> Many of the computer systems involved are crucial to a business's
> operation; some are critical to human life. The potential (and in some
> cases the actuality) is there for major losses from disruption of
> service and theft. The hackers are unknown outsiders in whom a serious
> organization can place no trust whatsoever.

One of my examples was Com-Share Incorporated. This description exactly fits Com-Share. Com-Share had only one buisness: Selling timesharing services. Com-Share had more customers than any other timesharing service in the early '70s, and the customers were distributed nationwide. Security was of the utmost importance; without it, the company would surely have failed in the marketplace.

In this context, the reward offered by Com-Share to anyone discovering a loophole in the system security served an important role. Goldstein describes the hackers who threaten a commercial service as follows:

> The hackers are unknown outsiders in whom a serious
> organization can place no trust whatsoever.

Without the reward, the company would have clearly had to react to hackers as the above quote indicates. With the reward, the company could not exactly trust hackers, but rather, the company could make it more rewarding for a hacker to tell the company what was wrong than to take a less desirable path such as selling improperly obtained information to a third party. A reward does not automatically make all hacking constructive, but it offers an incentive for constructive hacking. By the same token, legal dis-incentives for destructive hacking also can help.

What I oppose are blindly applied blanket actions taken against all hackers. These provide an incentive to stay away from hacking, but if someone insists on hacking, they provide no incentive towards constructive behavior. I feel that hacking is a sufficiently attractive activity that some people will hack whether it is legal or not, and we must keep incentives in the system to direct the behavior of such people to constructive ends.

Douglas W. Jones

Hacking the etymology

Nigel Roberts, D-8043 Unterfoehring <roberts%untadh.DEC@decwrl.dec.com>
Tue, 13 Dec 88 07:00:26 PST

The recent discussions of the etymology of the terms "hacker", "cracker", _et al_ & the recent spirited defence of the activity by one or two contributors (at least one of them being a self-confessed "hacker") has set me to thinking.

In RISKS & elsewhere, I see a "generation gap" between what, for want of a better term, I would describe as the "old-time hackers", who were experimenters, and the current cyberpunks, the "hackers" of popular mediaspeak, the eponymous "shatterers".

I think this apparent generation gap is fundamental to the discussion.

The "old-style hackers" (of whom I am vain enough to claim I belong) learned their computing in the 60s and 70s, often in a university or similar multiuser environment, where, as often as not, hacking involved programming.

Today's stainless steel rats are much more likely to have discovered computers in the home, courtesy of Apple, Commodore or IBM, and started their "network tourist" activities by purchasing a modem.

The old school (& I include myself here) resents the way the term "hacker" has been hi-jacked and is today being used to connotate anti-social activity. This is despite the ambiguous roots of the term (described by Weizenbaum in _Computer Power & Human Reason_).

Today's cyberpunks are computer burglars, who are attempting to justify their activities by claiming a common motivation with their arguably less anti-social predecessors.

Like any story of generation conflict, there are elements of truth in the claims of both sides.

It is going to be impossible to prevent the media from using the word "hacker" in a way that the "old school" dislike. It would almost be easier to claim that the word "gay" meant "happy, carefree".

But maybe the media and the collective unconscious understand the evolution of hackerism better than we do.

For just as there is at least a tiny thread of commonality with the hackers of old in the network rats of the 80s, and I would say that there was some small element of today's network rats in the hackers of old.

But of course, there IS a distinction between hacking around a system whose sole reason of being is to teach people about computers, and hacking into systems which are being used for serious business purposes and where outsiders no right to be.

That difference is ethical, and has well expounded here in RISKS already.

Seeing as we can't get rid of "hackers" in the popular media, I would like to coin the term "punk hackers" (an abbreviation of 'cyberpunk hackers') to describe their anti-social activities.

It seems to fit only too well, just like "punk rock" is rock music with swearing & spitting at the audience.

And using it would let us "old hackers" keep our self-respect!

Nigel Roberts, Munich, W. Germany.

Re: design intent of worm

Rich Thomson <thomson@wasatch.utah.edu>
Mon, 12 Dec 88 22:17:59 MST

In RISKS DIGEST 7.92 cjosta@taux01.UUCP (Jonathan Sweedler) writes
>It seems that Robert Morris Jr. would not have done anything illegal
>(even under these new bills) if his virus had worked as it was designed
>to work: to propagate quietly from machine to machine.

Several times I've seen it discussed here on RISKS about what the worm would have done had "it worked as it was designed to work". One of our local compiler gurus, Donn Seeley, was the person who decompiled the worm code from which Gene Spafford wrote his paper. Donn Seeley has also written a paper on the worm and I attended a talk he gave on the worm here at the University of Utah.

He was asked the question "On USENET there has been discussion to the effect that the author intended the worm to propagate slowly from machine to machine, but a programming error caused the worm to replicate out of control. What evidence did you see in the code to support this?"

His answer was "None." This business about the worm "doing what it was designed to do" is merely a rumor going around USENET and has no substantiation in fact, unless RTM himself starts claiming that there was a design mistake. Since RTM has so far remained silent, I'm inclined to believe Donn Seeley.

There is NO EVIDENCE in the decompiled code to indicate that the worm was intended to propagate slowly. In fact, the minimum lifetime the worm could have is fifteen minutes. There is code in the worm that deals with "population control", but this is oriented more towards making sure that not too many copies of the worm are running so that the worm can get some "work" done. Otherwise, the worm would never propagate out of the first few machines because it would be so busy re-infecting them.

-- Rich

It's NOT a computer!

<minow%thundr.DEC@decwrl.dec.com>
13 Dec 88 14:17

Reading the recent risks discussion (and listening to conversation at parties)
was an education. So much magic:

```
cr--r-----  1 root     sys       3,   0 Jan 10  1987 /dev/mem
chown root /dev/mem /dev/kmem ...
chgrp sys /dev/mem /dev/kmem ...
chmod 440 /dev/mem /dev/kmem ...
```

(From Paul McKenney's note in Risks 7.87)

Friends, this thing under my desk isn't a computer, and I'm not a computer
programmer. Of course, it looks like a computer, and the woman who services
it probably assumes it's a computer, and the guy in the next office who
designed it is quite certain it's a computer, (and the folks who pay
my salary hope I'm a computer programmer), but they're all wrong.

It's a tool, that's all; and, when I'm reading my mail or writing my programs,
I'm every bit as naive as the folks who say "hello" when the login program
tells them to. It's a smart typewriter, and that's all it should be.

I don't want to program my workstation. I don't want to become a Unix guru
to get my work done, and I don't want to have to play hide-and-seek with every
snake to slither out of a C programming course. I want to take the stuff out
of the box, plug it in, and get some work done without having to worry whether
/dev/mem is owned by root.

Telling me how to repair the problem is missing the point altogether.
In fact, there is so much software inside of that workstation and the
comptuter network it connects to: Ultrix, X-windows, Microemacs, Ethernet,
VMS, more Ethernet, disk servers, and whathaveyou, that I doubt that there
is any single person who can navigate through the entire collection. I have
to trust the people who have "privileges" to do their job responsibly, and
the people who design the systems to limit my risk.

Now, where did I put my copy of Normal Accidents?

Martin Minow
minow%thundr.dec@decwrl.dec.com

The above does not represent the position of Digital Equipment Corporation.

There's no excuse

<minow%thundr.DEC@decwrl.dec.com>
13 Dec 88 13:58

Excerpts from an op-ed piece in the business section of the Boston Globe,
Tuesday, Dec 13, 1988:

> For Robert T. Morris Jr., hacker, there's no excuse
> By Aaron Harber

[Harber teaches at the Kennedy School of Government at Harvard University and is a director of two software companies.]

... With hackers around the country proclaiming Morris a superstar, he is on the path to becoming a folk hero. We must see that his punishment is swift and severe so that his actions are immediately seen and understood as undesirable and unacceptable. To do any less will sow the seeds for further undertakings by those who are as "bright and bored" as Morris.

... Morris' good intentions failed in two respects. First, once he realized his error, he had many opportunites to correct it... He panicked and failed to seriously attempt to correct his monster.

More importantly, Morris knew he should not have made the attempt at all. It was not only that something might go wrong. He had many other ways of proving his theories and, ironically, was someone people would listen to had he raised the concern in a legitimate forum. In a supervised demonstration, he could have made his point and received the attention and accolades he may have sought.

His attempt was based on the premise accepted by far too many people: Computer systems are different from other forms of property... It is considered by all to be unethical and illegal to enter someone's business and examine records without permission.... Yet hackers see invasion of a system as a challenge and are often rewarded for their "successes."

... Students are taught skills that give them the power to do both positive and negative deeds, yet they are rarely, if ever, schooled in the ethical deployment of that power. Given the constant demonstrations of a hacker's potential power, why are computer ethics courses not mandatory? ...

Robert Tappan Morris Jr. is an example of how we have failed and his example is one that will be followed until we change society. Hackers will continue to see breaking into systems and implanting viruses as a game. They know they would not physically ever harm someone, yet do not comprehend the violence of their seemingly benign actions. They rarely see, in person, the results of their activities and this distance promotes their insensitivity.

... The possibilities [for harm] are endless. Unless and until new standards are set and accepted by the country, we will continue to suffer from people such as Robert Tappan Morris Jr. and their computer viruses.

[Excerpted by Martin Minow minow%thundr.dec@decwrl.dec.com
The above does not represent the position of Digital Equipment Corporation.]

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 94

Thursday 15 December 1988

Contents

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

Vincennes: conclusively, a computer-related error

"Clifford Johnson" <GA.CJJ@Forsythe.Stanford.EDU>
Wed, 14 Dec 88 21:07:08 PST

> From: davis@wheaties.ai.mit.edu (Randall Davis)
> When [Vincennes] first happened we saw a remarkable flood of
> messages to Risks speculating about the role of advanced
> automation in general and computers in particular as central
> to this disaster....
> there is, with only a few exceptions, clearly a strong
> desire in the Risks community to believe otherwise. Perhaps
> that's worth a few minutes reflection.

I reflect that *all* the information that panicked the Vincennes crew and captain came from the computers. The captain was not faulted for trusting his AA officer, the AA officer was not faulted for misreading (or not reading) his console, and the officers who reported to the AA officer were not found at fault. 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. Replacing alphanumerics with an up/down arrow is the planned solution to the Vincennes problem. (Who will be accountable if the arrow is misread, or if it points the wrong way owing to a subtle bug - again the computerization?) As the OTA reported with respect to nuclear launch under attack (i.e. on warning): "The risk of error for an LUA system would seem highest when the human being's ability to make highly structured errors combines with the machine's limited ability to correct [for] them." (1981, MX Missile Basing.)

I saw a front-page report of the approbatory celebration that greeted the Vincennes Captain and crew on their return to port. Garlanded and with a huge grin on his face, having been exonorated by the official inquiry, Captain Rogers stated he knew he'd done the right thing in the circumstances. I chillingly wonder if the sister ship, that correctly identified the Iranian jet as commercial, will receive as loud applause?

Ethics

"Dennis G. Rears (FSAC)" <drears@ARDEC.ARPA>
Wed, 14 Dec 88 12:37:49 EST

Several articles in Risks and other USENET groups have commented on the need for ethics course(s) for "computer people". I feel there is a need for them, however, I question the content. It is my belief that what is and is not "ethical behaviour" is not clearly defined. There are some areas that are agreed on as off limits, "destroying data" and some which are not "perusing files". In my mind I don't have a clear guide. It's like the one Supreme Court Justice who said "I can't define Pornography but I know it when I see it". I think that describes computer ethics right now.

Also on a similiar theme, the system admins who were complaining about the loss time involve in fighting the worm should have had their systems right in the first place. I view it as negligent to have programs like uucp & sendmail on systems unless the admin is aware of all the ramifications. They didn't deserve to have their systems broken into, but, they didn't really do their job in the first place. I must add this does *not* apply to victims of the worm.

The risk I see is blind trust in computer jocks (wizards, gurus, experts, etc). The trust being mainly in technical compentence. I have seem some sysadmins who are nothing more then operators (some even less). However at many places non-computer people believe "oh, the problem so technical I won't explain to you because you won't understand it". As part of being a professional we must spread our knowledge and give other a deeper understanding on what know and do.

Dennis Rears

"It's already in the computer"

David Sherman <dave%lsuc%attcan@uunet.uu.net>
13 Dec 88 10:01:21 EST (Tue)

The other day I parked in a multi-story parking lot while going to the doctor. "Parking rates: $1.00 per half-hour". Well, it took several minutes to get to a parking space on the 6th floor, and about 10 minutes to drive down to the cashier when I came out; this included a good 7-8 minutes waiting in the line of cars to pay the (single) cashier.

My in-ticket was stamped 15:09. I decided while waiting in the line of cars to leave, around 16:08, that as a question of principle I shouldn't pay for more than an hour, since I was parked for a fair bit less than an hour. I make it to the cashier (where they have a "5 minutes grace" notice), and it's 16:15 when he punches in my ticket. I hand him $2, and he insists I owe him another dollar. I say no, pointing out the amount of time I was waiting in the line to pay.

The RISKS interest lies in his response at this point.
Before computer control of parking cashiers, he could no doubt have waved me off and accepted the $2. Now, though, "it's already in the computer", and if he doesn't get $3, he tells me, it'll come out of his pocket. I hung tight, on principle, and told him to take my number and have his supervisor call me if he liked (he didn't like). Since I was blocking the only exit to the lot, cars were backing up behind and people were getting annoyed, eventually he gave up and raised the gate.

So who controls how much you owe at a parking exit? People don't matter. It's "the computer".

David Sherman, Toronto attcan!lsuc!dave@uunet.uu.net

RISKS of Tightening Security

"F.Baube" <fbaube@note.nsf.gov>
Wed, 14 Dec 88 10:12:14 -0500

The _City Paper_ of Washington DC, December 9, reports that the _Washington Times_ was stricken by a "computer catastrophe" last week. No, not a mainframe felled by a virus infection.

"The powers-that-be at the _Times_ disabled the computer system's powerful "RODI" command.

The RODI command ("Read Only Direct") was much loved by _Times_ reporters and editors because it permitted anyone with a computer logon to examine practically any file - stories or notes - in the ... system. Only files that bad been secured with the system's "lock" command were safe from the eyes of the RODI cognoscenti. Because the lock command is so cumbersome, 99.9% of the paper's files were left unguarded.

"Everyone thought it was their personal little secret," one computer investigative ace says. "On Wednesday [Nov. 30] you could hear an audible wave of despair washing over the newsroom ... One _Times_ reporter ... lamented aloud: "How am I supposed to know what's going on around here without RODI ?"

Nosy _Times_ reporters aren't the only ones crushed by the loss of RODI. _Times_ sports fans are despondent, too, because RODI allowed them to freely scroll the sports wire for scores and news.

One _Times_ employee blames this column for RODI's termination, saying, "I'm sure the editors got tired of seeing their memos printed in _City Paper_."

#include <disclaimer.h>

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 95

Friday 16 December 1988

Contents

- Armed with a keyboard and considered dangerous
  Rodney Hoffman
- Value for money? (Part 2)
  Jerry Harper
- USAF software contractors score poorly
  Henry Spencer
- Reasoning about software
  Nancy Leveson
- Hacking the etymology
  Nigel Roberts
- [Shattering revelations]
  Shatter
- Info on RISKS (comp.risks)

Armed with a keyboard and considered dangerous

Rodney Hoffman <Hoffman.es@Xerox.com>
16 Dec 88 08:13:25 PST (Friday)

The 16 Dec 88 'Los Angeles Times' contains this story (excerpts only):

EX-COMPUTER WHIZ KID HELD ON NEW FRAUD COUNTS
By Kim Murphy

Kevin Mitnick was 17 when he first cracked Pacific Bell's computer system, secretly channeling his computer through a pay phone to alter telephone bills, penetrate other computers and steal $200,000 worth of data from a San Francisco corporation. A Juvenile Court judge at the time sentenced Mitnick to six months in a youth facility....

[After his release,] his probation officer found that her phone had been disconnected and the phone company had no record of it. A judge's credit record at TRW Inc. was inexplicably altered. Police computer files on the case were accessed from outside.... Mitnick

fled to Israel. Upon his return, there were new charges filed in Santa Cruz, accusing Mitnick of stealing software under development by Microport Systems, and federal prosecutors have a judgment showing Mitnick was convicted on the charge. There is, however, no record of the conviction in Sant Cruz's computer files.

On Thursday, Mitnick, now 25, was charged in two new criminal complaints accusing him of causing $4 million damage to a DEC computer, stealing a highly secret computer security system and gaining access to unauthorized MCI long-distance codes through university computers in L.A. and England.

U.S. Magistrate ...took the unusual step of ordering [Mitnick] held without bail, ruling that when armed with a keyboard he posed a danger to the community. "This thing is so massive, we're just running around trying to figure out what he did," said the prosecutor, an Asst. U.S. Atty. "This person, we believe, is very, very dangerous, and he needs to be detained and kept away from a computer." LA and FBI Investigators say they are only now beginning to put together a picture of Mitnick and his alleged high-tech escapades. "He's several levels above what you would characterize as a computer hacker," said Detective James K. Black, head of the LA Police Dept's computer crime unit. "He started out with a real driving curiosity for computers that went beyond personal computers.... He grew with the technology."

Mitnick is to be arraigned on two counts of computer fraud. The case is believed to be the first in the nation under a federal law that makes it a crime to gain access to an interstate computer network for criminal purposes.... Federal prosecutors also obtained a court order restricting Mitnick's telephone calls from jail, fearing he might gain access to a computer over the phone lines....

Re: Computer Virus Eradication Act of 1988

Les Earnest <LES@SAIL.Stanford.EDU>
16 Dec 88 0103 PST

The note from Don Alvarez <boomer@space.mit.edu> in RISKS-7.91 gives the text of proposed legislation that is intended to inhibit certain kinds of computer crime. If you look at it only as a protection against skulduggery then it looks reasonable, but it also seems to prohibit certain plausible defensive tactics against software piracy.

Suppose that a software developer wishes to protect his program against theft and happens to know with certainty that the computing environments of all customers will have a certain property and that those of thieves may not have that property. It would be reasonable to have the program check for the property and, if it is missing, either self-destruct or malfunction in subtle ways. (Admittedly there is some risk in doing this, given all the crazy things that customers do, but with suitable admonitions this could be a reasonable defensive tactic. In fact it has been used in the past.)

The proposed legislation reportedly says:
"(a) Whoever knowingly-
"(1) inserts into a program for a computer information or commands,
knowing or having reason to believe that such information or commands
will cause loss to users of a computer on which such program is run
or to those who rely on information processed on such computer; and
"(2) provides such a program to others in circumstances in which those
others do not know of the insertion or its effects; or attempts to do so,
shall if any such conduct affects interstate or foreign commerce, be fined
under this title or imprisoned not more than 10 years, or both."

This wording, as it stands, would appear to make defensive programming of the type described above illegal. The problem is that it fails to distinguish between the interests of legitimate users of programs and those who steal them.

-Les Earnest

Value for money? (Part 2)

Jerry Harper <jharper@euroies.UUCP>
Tue, 13 Dec 88 20:43:11 GMT

Just a week back a note appeared from me citing an Irish Times report of how our Department of Health spent approximately $67million on a medical informatics system which was substandard in many respects. A lamentable fact of the debacle is the Dept's dogged refusal to accept the advice of a range of academics concerning inadequacies in the system. This little anecdote will impress RISKS readers I hope.

Shortly, after the contract had been agreed, one of the management consultants favouring the system because of its advanced features had the temerity to ring one of the opposed academics and ask if they could recommend a good introduction to medical information systems!

USAF software contractors score poorly

<attcan!utzoo!henry@uunet.UU.NET>
Wed, 14 Dec 88 01:39:45 EST

>From the Nov 14 Aviation Week & Space Technology (page 103):

The [USAF] Electronic Systems Div. has developed a new system for Air Force source selection boards to use to evaluate contractors' software capabilities. Using a questionnaire, companies are ranked from one to five. Some 84% of the 178 contractors checked so far rank at the lowest level, with chaotic or unpredictable, poorly controlled processes. Only 14% ranked at the second level, meaning they could repeat previously mastered tasks. Two percent met the third level with well-understood processes. The processes for the fourth

level are defined as well-measured and controlled, and for the fifth as optimized. So far no contractor has ranked above the third level.

---

reasoning about software

Nancy Leveson <nancy@sablon.ics.uci.edu>
Fri, 16 Dec 88 11:55:44 -0800

I have a somewhat different interpretation of the draft ICAO standard than Steve.

I originally quoted from a draft standard that included the following:
> "... [Software] must be developed systematically in such a way that its
> behavior, under all possible conditions, can be established by logical
> reasoning (to a level of formality appropriate to the application).

Steve responded with:
<> It's my opinion that strict enforcement of the above requirement simply
<> makes the developer liable for errors, but doesn't do much for actually
<> improving software reliability. It is unlikely that "all possible
<> conditions" can be for[e]seen, let alone provided for. The problem becomes
<> bigger as the complexity of the system increases, to the point where
<> exhaustive analysis of a system could take centuries to perform.

One of the most effective ways to increase reliability is to decrease complexity. I have seen safety-critical systems where the developers purposely simplified their systems to make the above reasoning possible. The results were highly reliable. I believe (and have heard those in the field of formal verification confirm) that one of the advantages of formally verifying software is that it encourages simplicity in the software design in order to perform the necessary logical reasoning.

Reasoning about all conditions is currently required for hardware. System safety engineers use techniques such as FMECA (Failure Modes, Effects, and Criticality Analysis, as mentioned in the standard) to accomplish this. Should regulatory agencies relax their standards for the software used to replace this hardware? Such hardware analyses currently do find many problems that are fixed before they can cause an accident.

Microwave landing systems are used when visibility does not allow the pilot to land the plane alone. Current systems allow landing only when visibility is at least 200 feet, so the pilot has a chance to abort and go around. However, they are now talking about allowing landings where the visibility is zero. Perhaps we should not be putting trust in these systems if we cannot build them in such a way that we CAN reason logically about their behavior under all conditions.

<> The requirement is essentially that systems be perfect. That goal has
<> proven elusive (unattainable?) in all areas of human endeavor. Extensive
<> formalism and verification should be required of critical systems, but
<> requirements for perfect function are inane.

I don't read the requirement as requiring perfection. It says that we must build the software in such a way that we can reason about it under all conditions, including presumably what happens when there are software errors. The standards certainly should not imply that failures in such systems are acceptable. Would you want a standard involving the safety of commercial aircraft to require less than perfection? Extremely high reliability requirements (e.g., 10^-9 probability of failure over a fixed period of time) are merely attempts to provide virtual perfection in hardware systems where failures are random. In fact, it has been written that the FAA 10^-9 figure is meant to be equivalent to: "is not expected to occur within the total life span of the whole fleet of the model." [Waterman, "FAA's certification position on advanced avionics," AIAA Astro. and Aero., May 1978, pp. 49-51]

<> A better approach would be to require independent performance monitoring
<> and evaluation as part of the complete system.

I agree, but I don't think the standard precludes this; in fact, I read it as implying the necessity for it. However, independent performance monitoring and evaluation can be flawed and implemented imperfectly also; error detection can be quite difficult in many applications. I would feel most comfortable if companies do everything they can to make such safety-critical software as good as possible and then provide safeguards in case they had not been completely successful; both of these things need to be done in order for us to have the maximum confidence in our software at our current level of technology.

Hacking the etymology

Nigel Roberts, D-8043 Unterfoehring <roberts%untadh.DEC@decwrl.dec.com>
Tue, 13 Dec 88 07:00:26 PST

The recent discussions of the etymology of the terms "hacker", "cracker", _et al_ & the recent spirited defence of the activity by one or two contributors (at least one of them being a self-confessed "hacker") has set me to thinking.

In RISKS & elsewhere, I see a "generation gap" between what, for want of a better term, I would describe as the "old-time hackers", who were experimenters, and the current cyberpunks, the "hackers" of popular mediaspeak, the eponymous "shatterers".

I think this apparent generation gap is fundamental to the discussion.

The "old-style hackers" (of whom I am vain enough to claim I belong) learned their computing in the 60s and 70s, often in a university or similar multi-user environment, where, as often as not, hacking involved programming.

Today's stainless steel rats are much more likely to have discovered computers in the home, courtesy of Apple, Commodore or IBM, and started their "network tourist" activities by purchasing a modem.

The old school (& I include myself here) resents the way the term "hacker" has been hi-jacked and is today being used to connotate anti-social activity. This is despite the ambiguous roots of the term (described by Weizenbaum in _Computer Power & Human Reason_).

Today's cyberpunks are computer burglars, who are attempting to justify their activities by claiming a common motivation with their arguably less anti-social predecessors.

Like any story of generation conflict, there are elements of truth in the claims of both sides.

It is going to be impossible to prevent the media from using the word "hacker" in a way that the "old school" dislike. It would almost be easier to claim that the word "gay" meant "happy, carefree".

But maybe the media and the collective unconscious understand the evolution of hackerism better than we do.

For just as there is at least a tiny thread of commonality with the hackers of old in the network rats of the 80s, and I would say that there was some small element of today's network rats in the hackers of old.

But of course, there IS a distinction between hacking around a system whose sole reason of being is to teach people about computers, and hacking into systems which are being used for serious business purposes and where outsiders no right to be.

That difference is ethical, and has well expounded here in RISKS already.

Seeing as we can't get rid of "hackers" in the popular media, I would like to coin the term "punk hackers" (an abbreviation of 'cyberpunk hackers') to describe their anti-social activities.

It seems to fit only too well, just like "punk rock" is rock music with swearing & spitting at the audience.

And using it would let us "old hackers" keep our self-respect!

Nigel Roberts, Munich, W. Germany.

[Shattering revelations]

Shatter <unido!altger!Shatter@uunet.UU.NET>
15 Dec 88 04:58:42 MEZ (Thu)

First of all I would like to thank all the ppl who gave me feedback on my previous contribution to risks it has on the whole been quite positive :-)
[You will now have gathered that I have gone legit as I am now too well known to continue with active hacking and will have to make do with the odd foray into the net on highdays and holidays]. But there has been at least one recent contributor who does not seem to get the point that I was trying to make

and s my last effort was knocked up in 10mins I have decided to put a bit more effort into this one.
My previous article [if you can call it that] was not trying to justify anything
but was written to try to point out a major flaw that exists in the IT community
and it is one that should at least show some signs of being rectified in the
near future or more serious attacks on networks such s internet will no
doubt occur.
The contributor who compared modern day hackers to the punk rock musicians
of the 70's obviously has not spent time within the hacker community
in the last 10 to 20 years as if he had he would releise that the sense of
ethics and morality is as strong if not stronger than in his day
and his assumption is like saying all black male teenagers are muggers,
rapists and murderers.[but i wander yet again]
and I would like to say to him am I anyless of a caring,moral and intelligent
human being becoz I learned my craft on a home micro,network of tandy modal 80's
and a modem I made myself? Wot I think we have witnessed in recent issues of risks
is a kind of computer snobbery that does little to promote the spirt of goodwill
and intellectual exchange that should exist within our community [for all our sakes]. Comments have been made that
Hackers of today do not inform the owners
of the systems of the holes that exist and in some instances that is true but
I ask you "When those of you who claim to be 'old-time hackers' found a possible
security breach on a machine did you immdiatly go running printout in hand to
the owner of the system?????" I think not the temptation to explore just that little bit further is too great.
and in some cases the administrator is rude and often downright abusive
when a security hole is brought to his attention [sorry I am not sexist the masculine gender is used to mean mankind in general not just the male sex]
Which is often the case on commercial sites[an exparience I myself have
expirienced]
To finish this "article" off i will just make the following points:-
1. Can we please have less of this snobbery that exists
2. Work with the hacking community as much as possible. We will both gain
from the exparience [offer an insentive if nessesary[an account that is open to
all but only usable at nite and has say a MUD on it or even MONEY :-)]]
3. Work with each other

and finally if anyone has a need for any help with any thing that you
think I can help with then mail me at ...!unido!alter!Shatter and
i will see if I can help.
Shatter

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 96

Tuesday 20 December 1988

Contents

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

Soviets Claim Computer-Virus Shield

Peter Neumann <neumann@csl.sri.com>
Mon, 19 Dec 1988 13:15:45 PST

The Soviet Union said yesterday that so-called computer viruses have invaded systems in at least five government-run institutions since August, but Soviet scientists say they have developed a way to detect known viruses and prevent serious damage.

In August 1988, a virus infected 80 computers at the Soviet Academy of Sciences before it was brought under control 18 hours later. It was traced to a group of Soviet and foreign schoolchildren attending the Institute's summer computer studies program, apparently resulting from the copying of game programs.

Sergei Abramov of the Soviet Academy of Sciences claims they have developed a protective system, PC-shield, that protects Soviet computers against known virus strains. It has been tested on IBM computers in the Soviet Union. "This

protective system has no counterpart in the world," he said (although the details remain a state secret).

[Paraphrase of a UPI item in the San Francisco Chronicle, 19 Dec 88, p. A16]

UNICEF Belated Greetings

David Andrew Segal <dasegal@brokaw.LCS.MIT.EDU>
Sun, 18 Dec 88 13:02:52 EST

From the New York Times, Saturday, December 17, 1988

A computer problem has brought frustration instead of glad tidings to hundreds of people who ordered Unicef Christmas cards through the organization's toll-free telephone number. Many orders have been delayed or lost.

"We have a little bug in the system," said Colin J. Rainsbury, vice president of the greeting-card division ....

Unicef's direct-marketing manager, Laura A. Colassano, said the organization had processed more than 90,000 orders in the United States for the cards, ... She said almost 1,000 people had called about missing orders.

TMI Inbound Inc., a telemarketing agency in Omaha, receives orders from customers who call 800-FOR-KIDS and transmits the orders to BSA-Fulfillment Service Inc. in Lakewood, N.J., which fills the orders. "There's a problem with the computers speaking to each other," Ms. Colassano said.

[info about refunds...]

David Andrew Segal, Laboratory for Computer Science, MIT

[Also contributed by Chris Koenigsberg

Computer Ethics or just Ethics

David Clayton <LCO101@URIACC.BITNET>
Tue, 20 Dec 88 08:18:38 EST

There is a recent book titled "Everything I Need to Know I Learned in Kindergarten". I've only read excerpts and this is not a book review but I thought of the title as I was reading many contributors' comments regarding ethics for computer users. What I find interesting is the implicit assumption that a different (higher? lower? more stringent? more lenient?) set of ethics apply to those who by chance or choice work with computers. Apparently, because I use a keyboard and stare at a VDT, the rules of right and wrong, the definitions of proper -vs- improper behavior that were taught me as a child no longer apply. For some reason my choice of a profession has somehow rendered obsolete those rules I (we?) learned in kindergarten about respecting others and not taking what isn't ours.

We make attempts to wrap common snooping in terms of honor by making claims of

"respecting data" and "exercising the system" to find bugs and point out weaknesses in design and implementation. And we ignore or dismiss acts of thievery and vandalism by faulting the designers and administrators of pilfered systems. There is no doubt that systems must be secure, but we don't tear down the prisons because we can't build thief-proof banks. Courses in computer ethics may be an interesting forum for the discussion of ideas but let's not kid ourselves that these problems are so unique (and by association, we are so special) that we must be treated differently and so develop a new ethos.

David Clayton; Academic Computing; University of Rhode Island

The opinions are my own. I don't know what, or if, the University thinks about these things!

Those Who Do Not Learn From History ..

"F.Baube" <fbaube@note.nsf.gov>
Mon, 19 Dec 88 18:04:34 -0500

Some old mail, from one year ago .. Mr Patterson can hardly be blamed for not foreseeing what no-one else on the Internet did, either ..

And, what does 1989 have in store for Netland ?

------- Forwarded Message

Date: Mon, 21 Dec 87 15:22:26 EST
From: Ross Patterson <A024012%RUTVM1.BITNET@CUNYVM.CUNY.EDU>
Subject: IBM Christmas Virus

>Subject: IBM Xmas Prank {RISKS 5.79}
>(5) Is the Internet similarly vulnerable ?

Not to this one. It plays on several things that the Internet doesn't have:

1) A large number of IBM VM/CMS systems. The program would only run in a CMS environment. There is no reason one couldn't write something similar in any other language, though.

2) A suitable file transfer system. FTP doesn't apply. It must provide a way for a user to receive an unsolicited file, in a runnable form.

3) A good method of determining targets. The CMS NAMES and NETLOG files provided an excellent source of information. I suppose in a Unix environment, ".alias" and "/etc/aliases" would be ok, but .alias is comparatively rare, while NAMES files are almost universal in CMS.

Browsing this message is no fun at all. Just type Christmas ..

------- End of Forwarded Message

Re: Armed with a keyboard and considered dangerous

"F.Baube" <fbaube@note.nsf.gov>
Mon, 19 Dec 88 12:03:36 -0500

Rodney Hoffman (quoting a news article):
> [..] Federal prosecutors also obtained a court order restricting
> Mitnick's telephone calls from jail, fearing he might gain access
> to a computer over the phone lines....

.. and presumably he would whistle at 1200 bps.

Re: Computer Virus Eradication Act of 1988

David Keegel <munnari!murrumbong.cs.mu.oz.au!djk@uunet.UU.NET>
Tue, 20 Dec 88 17:11:03 EST

In Risks 7.92, Jonathan Sweedler wrote:
] In other words, can I break into any computer I want to and look at
] whatever files I want to, as long as I announce I'm there and don't
] cause any harm? Why do these laws center on causing harm to computers
] and not just illegal/unauthorized entry?

I think we need to be a bit more careful about what "harm" or "loss" means. For instance, if someone reads your private files, you can say that you have lost some of your privacy. If someone infects your computer with a "benign" worm/virus whose only effect is to use a few kilobytes of disk and some CPU time, you can still claim loss of processing power (assuming someone was using the machine).

When taken literally, this could even apply to such things as remote fingering: information is given to the finger program which causes it to use CPU time on another system. It seems that this cannot be called "loss" otherwise by running a non-optimised program I am potentially depriving others of processing power.

On the other hand, to say that loss means loss of data (files) allows a {h,cr,sn}acker to run a program that may crash your machine. Is there a clear dividing line between this and using 100% of the CPU? Where could we draw such a line?

I believe it _is_ important to avoid making laws which prohibit _all_ unauthorised access. Apart from questions about the fuzziness of the word "authorised" (eg: who is authorised to use "login"?), the important problem is that you do not allow people to test your security, without previous authorisation (try to imagine a one-man, part-time "tiger team" :-).

The possible advantages of "hack attacks" and the like have been covered before, so consider another facet of this: imagine that Joe User (joe@host)

one day mistypes his login name and discovers, by accident, that jo@host has no password required. He is dropped into Jo Bloggs' shell, without authorisation from her. Already he has broken the law.

Now (the interesting part), he is faced with the following dilemma: does he tell jo@host or root@host of this security problem, and face being charged; or does he keep his mouth closed about the situation? There is now a definite DISincentive to informing the sysadmins that jo has no password.

As if this weren't bad enough, imagine the hypothetical law made no distinction between "unauthorised use" and "harm". Since he has already broken this law, he may as well play around. For instance, to erase indications of his presence. Or to see who Jo is, and what she is doing.

Admittedly, this is a contrived situation which is highly unlikely in practice, but the point is that it is possible to use someone else's account, with absolutely _no_ malicious intent and yet become a criminal. A more realistic example is the person who is bored waiting for a print-out, and tries a few <user,password> combinations, or someone exploring some outside system to see what they can find out about it.

I contend that any legislation must not only charge the guilty, but also avoid charging the innocent.

David Keegel (djk%munnari.oz.au@uunet)
"Flattery will get you nowhere, unless someone else does it to you"

Manslaughter caused by computer error

<WWTMHJW@HEITUE5.BITNET>
Mon, 19 Dec 88 18:04 N

* * * Software bugs and copyright -- is the author a (re)liable owner? * * *

Six years ago, the Dutch journal Computable reported a case of manslaughter, attempted manslaughter, and attempted suicide in Western Germany caused by a computer error.

A print-out error caused a medical insurer to convince a 54-year old woman that she suffered from a fatal form of syphilis, and that she had transmitted the disease to her children; in panick, she strangled her 15-year old daughter and tried to kill her 13-year old son. The boy escaped, and succeeded in preventing his mother's death from a drugs overdose. The Duesseldorf court dismissed the accusation of murder, laid all blame with the computer error, and declared the woman unaccountable for her actions. It is not known whether any civil liability action followed this tradegy.

Two years ago, a software bug in a (canadian) radiation therapy machine in Texas caused a number of fatal accidents due to a radiation overdose (cf. Datamation, May 1987).

It seems that such (re)liability factors were partly responsible for the recent

withdrawal of all software protection proposals in Dutch Bill 19.921 on Combating Piracy of Copyright Works, after which the Bill was passed by the Dutch House of Representatives on 8 November 1988. In effect, the software clauses proposed to exclude so-called "computer programs" (otherwise undefined in the Bill) from the Dutch equivalent of Section 107 USC ("Fair Use"), under inclusion of a clause rather similar to Section 117 USC. Unfortunately, insufficient attention was given to morally acceptable activities as licenced under anglo-american Fair Use / Fair Dealing (including "reverse engineering" and analysis in either a profit or not-for-profit context). In fact, the Bill attempted to use copyright law for creating trade-secret protection on software, as was the case with the French and West-German Copyright revisions of 1985.

Also, it was proposed that programs should have a sufficient PERSONAL creativity level under the standard doctrine of Dutch case law for copyright protection. This caused quite a debate since legal entities may not qualify for title to "authorship" under such circumstances unless special agreements are drafted between employer and employee, in view of the moral (personal) rights under the Berne Copyright Convention (the Universal Copyright Convention does not recognize any moral rights). If software can be viewed as a "writing", no personal creativity requirements exist under the Dutch "copijreght" doctrine, and the Minister of Justice seems to have desired to elicit a fundamental debate on "copyrights" for legal entities versus "author's rights" for natural persons.

At present, the discussion evolves around the June 1988 Green Paper of the Commission of the European Communities on "Copyright and the Challenge of Technology", in which a number of questions are posed on all kinds of copyright works including software and databases. Important issues are (a) the relation between software property rights under the pending European Directive on Software Protection versus software (re)liability under the 1985 European Directive on Product Liability, and (b) to what extent a legal entity may claim "author's rights" under the Berne Copyright Convention with its strong emphasis on moral rights for natural persons. In short: is software an impersonal "product" to be protected under industrial property law, or a personal "service" to be protected under intellectual property law?

Unlike the anglo-american "work-for-hire" rule, a legal entity's title to authorship has been a hotly debated issue in continental-european intellectual property law, pursuant to section 27(2) of the Universal Declaration of Human Rights (New York, 1948) and to section 15(1)c of the International Covenant on Economic, Social and Cultural Rights (New York, 1966). During last year's "Tripartite Meeting on Salaried Authors and Inventors" organized by the International Labour Office in Geneva, no agreement could be reached on this issue.

If the natural author is the legal author under the Berne Convention, it stands to reason that he is also liable for any errors caused by "his" work, notwithstanding his employer's title to (and liability for) the pure information/ideas underlying "his" work. Here, the relation between (objective, impersonal) information/ideas/contents which are NOT protected under traditional copyright and the form/expression of the work which are protected under copyright is at stake, and it is of interest that recent publications in the field of intellectual property law attempt to shift the boarderline of copyright into pure information, despite the USA's First Amendment and various international in-

struments that purport to protect "Freedom of Information". From a liability point of view, this makes sense, since each individual is morally (and materially?) responsible for what he decides to publish, whether it is a highly personal recipe for making a nuclear device or an objective method fur curing cancer. From a scientific point of view, one may argue just the opposite. At any rate, private property rights and public information rights should remain in balance, as the Dutch events have demonstrated.

A paper "Going Dutch between Copyright and Droit d'Auteur" on some of these issues will appear in Computer Law & Practice (London) 5(1988)2 [special issue on the European Communities' Green Paper].

Herman J. Woltring

Study-committee on Software and Chips Protection, Netherlands Association for Computers and Law, wwtmhjw@heitue5.bitnet, na.woltring@na-net.stanford.edu

Biomedical & Health Technology Software Engineering Department
Eindhoven University of Technology Philips Medical Systems
The Netherlands The Netherlands

[A disclaimer indemnifying an employer or other party is not required under the Berne Convention!]

[The Duesseldorf case is in SIGSOFT Software Engineering Notes (SEN) 10 3 1985, and the Therac 25 radiation therapy case is discussed in SEN 11 3 and 12 3, 1986 and 1987, respectively.]

New EMI Shielding Material

<Boebert@DOCKMASTER.ARPA>
Tue, 13 Dec 88 13:56 EST

I just had an opportunity to examine a description and a sample of a new EMI shielding material called SAFENSHIELD from International Paper. This is a nonwoven fabric that looks a lot like the old "silkspan" we used to cover model airplanes in days of yore ... also the material teabags are made out of. The fabric has an embedded metallic substance which provides the shielding; can be put up like wallpaper, does not require bonding, and comes in two grades; the heavy grade is about $2.25 a square foot in small quantities, and is solderable. Attenuation specs look impressive. Brochure states that it is being used to shield Pontiac Fiero radios from ignition emissions. It must be a pretty new material because it is being sold from the corporate research center instead of a product division of International Paper. Point of contact in brochure is David Diermeier, (914) 577 7447. I don't know anything about this stuff except what is in the sales literature, but if it lives up to its specs it sure looks like a cheap and easy countermeasure to a variety of EMI RISKS.

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 97

Wednesday 21 December 1988

Contents

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

Software Safety report in UK

Philip Wadler <wadler@cs.glasgow.ac.uk>
Wed, 21 Dec 88 10:48:42 GMT

The following may be of interest to Risks readers. The message is from Jane Hesketh of Edinburgh Computing and Social Responsibility. -- Phil Wadler

>From jane@aiva Mon Dec 19 10:52:12 1988

Computer Weekly 15.12.88

"Software safety cannot be guaranteed, warns DTI"

A draft report for the Government on safety-critical software emphasises the impossibility of guaranteeing error-free programs, despite their widespread use to control aeroplanes and nuclear power plants.

Commissioned by the DTI and carried out by the Institution of Electrical Engineers and the BCS, the report has met with mixed reactions from the safety-critical software community.

One of the more ominous warnings contained in the report is that an entirely unambiguous specification is not strictly feasible.

"The uncertainty in our knowledge of the real world creates the potential for our specifications to be wrong, including being incomplete," the report states. " This is apart from any mistakes we may introduce when we come to describe the requirements in specifications".

The report is not describing remote safety-critical applications but ones already in operation. While Sizewell B will be the first UK nuclear power plant whose safety system is computer-controlledd, the safety of a nuclear plant on the NorthWest coast of France is already in the hands of software.

One of the criticisms of the draft report is that it is limited too closely to safety-critical software in the UK. The whole thing lacks a European perspective" says Robin Bloomfield, chairman of consultancy delard, which co-wrote the MoD safety-critical software standard 00-55. " For example, it should have included a current West German proposal for a standard to cover all industries".

Another criticism is that the report does not go far enough in trying to bring together safety-critial standards, which many in industry now feel to be diffuse and inconsistent.

"This document has not covered standards sufficiently," says David Youll, who is software engineering group manager at the Cranfield IT Institute.

Over-reliance on a single source of data

<cory@gloom.UUCP>
Fri, 16 Dec 88 17:13:11 EST

With all of this discussion on over-reliance on automation, an anecdote that a friend told me a while back came to mind. I though that it was appropreate to the current discussion.

Ed (the guy who told this to me) is a Master Chief Petty Officer (ret.). Part of his responsibilities included checking out new members of his squadron in the flight simulator. One of the pilots that he had to check out in the simulator was acting a bit 'cockey'. While the new guy was not looking, Ed disconnected the Artificial Horizon. (for those of you not familiar with airplane cockpits, this is a control that is used to inform the pilot of the current orientation of the aircraft about the X & Y axes (it doesn't tell direction). there are several other instraments that give the same data, notably the turn and bank indicator) The pilot took of (the simulator) and almost immediatly flipped over and crashed. He did this three times in a row. The reason? Over-reliance on a single channel of data input -- the Artificial Horizon. It showed the plane in a level

flight, while the turn and bank indicator showed the correct data.

This occured in a simulator. Nobody died as a result. It does illustrate what happens when humans (and computers for that matter) depend on a single source of data, and that source is spewing out bogus data (which can sometimes happen).

Other conclusions I will leave to you... this is too long already.

Cory Kempf UUCP: encore.com!gloom!cory

Computers vs Scandanavian Design

bobf@lotus.UUCP <Bob Frankston>
Wed Dec 21 07:49:41 1988

The Boston Globe had an article on the near demise of Scandanavian Design -- a 70 store furniture chain that was doing $100M/yr. According to the article what caused things to fall apart was an attempt to convert from an antiquated Honeywell system to a modern ($4.5M) IBM system.

The article also mentions a lack of senior management. The observation is that computers are not turnkey systems one just installs but they require an MIS staff with much expertise. The reason is not that computers are complicated but that they are integral to the operation of one's business.

While I expect that one will, in the future, buy systems that take care of the business and allow management to concentrate on the interesting aspects (whatever that might be for an individual), we need to make it clear that the current systems are idiot savants.

What is missing is a deep computer literacy that allows nonprofessionals (and many professionals in the field) to understand the computer as a component of a system. It is one thing to teach Basic in school, it is another to impart a deeper understanding of computation.

A trivial example was an office manager I had. I was implementing a property sticker system and wanted red permanent stickers and black removeable stickers. She did this, but both sets had the same numbers, she had assumed that a red 158 and a black 158 were different. While that may be true visually and could even be stored that way, it wasn't an effective distinction in such a system. What was missing was the concept of a unique ID.

Supercomputer used to "solve" math problem

Henry Cox <cox@spock.ee.mcgill.ca>
Wed, 21 Dec 88 09:23:26 est

BEYOND THE MIND'S POWERS - SUPERCOMPUTER CRACKS OLD MATH PROBLEM

[From the Montreal Gazette, 21 December 1988]

A team of Concordia University [another Montreal area university] computer scientists using a U.S. Defence Department supercomputer have solved a theoretical mathematics problem so complex that it is beyond the capability of the human mind to comprehend.

Clement Lam, who is a member of the matemetical computation division at Concordia's computer science department, said the complexity forces scientists to accept the supercomputer's solution more or less on faith. [The RISKS connection...]

This raises important questions about the power of computers and whether a proof that mankind cannot fully understand can be accepted. "This is one of the very important philosophical questions," Lam said. [A practical question as well, I think. How can we be sure the answer is correct if we can't check it?]

He added, however, that he is confident the mathematical problem faced by him and his colleagues "is solved".

The problem, first posed in the 18th century by a Swiss mathematician, deals with the question of whether a mathematical entity called a "finite projective plane of order 10" can exist.

Lam and three collegues, John McKay, Larry Theil, and Stanley Swiercz, concluded that such an entity cannot exist.

The problem deals with whether numbers and groups of numbers can be organized in a particular fashion. To discover the solution, concordial scientists had to search through more than 1,000,000,000,000,000 combinations of possibilities - or about 50,000 for every human being.

He said studying just one possibility would be like having the computer examine every combination and outcome of a chess move, but much more complex. The skill was is organizing and programming the computer.

[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]

Re: Armed with a keyboard and considered dangerous [RISKS-7.96]

Dan Franklin <dan@WATSON.BBN.COM>
Wed, 21 Dec 88 16:58:02 EST

F. Baube (commenting on a news article quoted by Rodney Hoffman in RISKS-7.95):
> > [..] Federal prosecutors also obtained a court order restricting
> > Mitnick's telephone calls from jail, fearing he might gain access
> > to a computer over the phone lines....
> .. and presumably he would whistle at 1200 bps.

Hardly. All he needs is a touch-tone phone.

First, it may well be possible to play games with phone service using only touch-tone phones; I could easily believe that each local phone exchange has a "secret" number that allows their employees to alter the characteristics of phone lines for testing purposes.

But more importantly, he could have set up a phone number in advance which

would allow him to use a touch-tone pad like a keyboard. (With 12 keys on the pad, two keypresses are sufficient to represent any ASCII character, including control characters.) Add text-to-speech equipment for the other direction, and he's all set.

Having been jailed before, he could easily have prepared for being jailed or otherwise kept away from keyboards again. This private line and the equipment need not be in his house or under his name, so there's no way anyone could be sure it wasn't available to him.

Dan Franklin

[Also noted by Deshler Armstrong <dela@ee.rochester.edu>]

Another article on the dangerous keyboard artist

LEICHTER-JERRY@CS.YALE.EDU <"Jerry Leichter>
Tue, 20 Dec 88 10:56 EST

"LOS ANGELES (UPI) - In a rare ruling, a convicted computer hacker was ordered held without bail Thursday on new charges he gained illegal access to secret computer information of Leeds University in England and Digital Equipment Corp.

Kevin David Mitnick, 25, of Panorama City, is named in two separate criminal complaints charging him with computer fraud. Assistant U.S. Attorney Leon Weidman said it is unusual to seek detention in such cases, but he considers Mitnick 'very, very dangerous' and someone who 'needs to be kept away from computers.'

U.S. Magistrate Venetta Tassopulos granted the no-bail order after Weidman told her that since 1982, Mitnick had also accessed the internal records of the Los Angeles Police Department, TRW Corp. and Pacific Telephone.

'He could call up and get access to the whole world,' Weidman said.

Weidman said Mitnick had served six months in juvenile hall for stealing computer manuals from a Pacific Telephone office in the San Fernando Valley and using a pay phone to destroy $200,000 worth of data in the files of a northern California company.

Mitnick later penetrated the files of TRW Corp. and altered the credit information of several people, including his probation officer, Weidman said.

He said Mitnick also used a ruse to obtain the name of the police detective investigating him for hacking when he was a student at Pierce College. He telephoned the dean at 3 a.m., identified himself as a campus security guard, reported a computer burglary in process and asked for the name of the detective investigating past episodes, Weidman said.

The prosecutor said Mitnick also gained access to the Police Department's computer data and has impersonated police officers and judges to gain information.

A complaint issued Monday charges Mitnick with using a computer in suburban Calabasas to gain access to Leeds University computer data in England. He also allegedly altered long-distance phone costs incurred by that activity in order to cover his mischief.

A second complaint issued Thursday charges Mitnick with stealing proprietary Digital Equipment Corp. software valued at more than $1 million and designed to protect the security of its computer data. Mitnick allegedly

stored the stolen data in a University of Southern California computer.

An affidavit filed to support the complaints said unauthorized intrusions into the Digital computer have cost the company more than $4 million in computer downtime, file rebuilding and lost employee worktime.

A computer operator at Voluntary Plan Assistance in Calabasas, which handles disability claims for private firms, told investigators he allowed his friend unauthorized access to the firm's computer.

From that terminal, Mitnick gained access to Digital facilities in the United States and abroad, the affidavit said."

Virus article debunked

Stephen Page <sdpage%prg.oxford.ac.uk@NSS.Cs.Ucl.AC.UK>
Wed, 21 Dec 88 20:15:21 gmt

A disappointingly journalistic article entitled "Rewriting the Book on Viruses" appears in the December 1988 edition of Computer Newsletter, a publication of the British Computer Society. It describes a talk from a Dr Alan Solomon, "who runs the only Data Recovery hospital in the world". Here are some extracts:

"... Solomon insists that viruses are actually extremely scarce. 'Viruses are very rare indeed. I'm getting about 1 or 2 reports a week which turn out to be genuine viruses. That's in a population of half a million computers,' estimates Solomon..."

"The biggest virus problem is misinformation, according to Solomon, who told the audience that 'everything you've read and everything you know about viruses is wrong'. He goes on to state an example, 'People are calling everything a virus. At the height of commotion, a couple of months ago, I had a person call in and say "I've got a problem, I think it's a virus. My printer won't print a pound sign."'"

"Viruses do not travel on executable disks, they spread on blank disks. Solomon warns, 'The real threat is data disks ... 99% of the time boot sector viruses are travelling on data disks.'"

"Solomon prescribes a few tips on preventative measures: get software from a reputable source, if a boot fails -- switch the computer off, stay informed and make a clean copy of DOS and write protect it."

There are two interesting flaws in this article:

1. No where in the article, with the sole exception of the word "DOS" in the extract above, does the author point out that the article defines "computers" to mean "machines of an IBM-PC architecture running the PC/MS-DOS operating system". Thus he dangerously misleads the reader into worrying about blank mainframe disks or, worse, into not worrying about executable disks on other machines.

2. His assertion that viruses are "extremely scarce" is incorrect for some hardware/software architectures, in particular the Macintosh.

I would not like to guess at a percentage, but certainly almost
every Macintosh user I have met has suffered from an nVir attack!

Disinformation is always dangerous. Perhaps RISKS readers need to arm themselves with a short nontechnical fact sheet for their colleagues who are interested in finding out what is really going on.
Has anyone written something simple along these lines, which we could show to people who find all the journalism confusing (or wrong)?

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

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

Volume 7: Issue 98

Thursday 22 December 1988

Contents

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

The Fetzer Paper in CACM

Brian Randell <B.Randell@newcastle.ac.uk>
Thu, 22 Dec 88 12:43:08 WET DST

The following message is intended to serve as a response to the comments by Nancy Leveson et al. (in RISKS-7.84) on our original brief message in RISKS-7.61 about Fetzer's paper. It is extracted from a much more detailed statement that will appear in the Communications of the ACM.

The furore that the article has aroused in the program verification community has caused us to go back and re-read Fetzer's paper more carefully, to see whether it really deserves the opprobrium which the program verification community has been heaping on it. Part of the problem seems to us to be the (unfortunately justifiable) fear that the paper will be misinterpreted by laymen, particularly those involved in research funding. We have good reason to sympathise with such reactions, given the misunderstandings that arose in some quarters from the Knight and Leveson paper on design diversity. Indeed, both papers demonstrate the care that needs to be taken in assessing how different readerships will react to one's writings. However we now believe that there are also significant philosophical issues underlying the present debate, which is not helped by the terms in which some of the reactions have been couched. [In our CACM paper, we go on and analyze one such issue, that caused by the difference between explanatory and evidential reasoning.]

In essence our view is that the dispute has arisen as a discrepancy between the program verification community's view of their practice and objectives on the one hand, and the outside world's view of those objectives on the other. It is in fact a public image problem, and public image is not to be corrected simply by the writing of intemperate letters. We suspect that a major underlying reason for the undesired image is that there has been a good measure of overselling of the concepts. (This is not of course the first occurrence of this practice in computer science, nor will it be the last.) A recent and all too clear example of this overselling can be seen, in the case of hardware verification, by contrasting exaggerated advertising claims for the VIPER microprocessor (e.g. "VIPER is the first commercially available microprocessor with both a formal specification and a proof that the chip conforms to it") with the careful and balanced discussion, in Avra Cohn's report on her (very impressive) work on formal verification of the VIPER `block model', of what was actually proven, and what was out of scope of the proving techniques. (The above advertisement is in fact quoted by Cohn, who rightly goes on to state that "such assertions, taken as assurances of the impossibility of design failure in safety-critical applications, could have catastrophic results".)

If our belief that formal verification has been oversold is correct, then articles such as `Program Verification - The Very Idea', misconceived though we now accept it undoubtedly is, might be seen in the longer term as providing a stimulus for a strategy of corrective measures necessary to counter the false sense of security that is, we fear, all too commonly promoted by vendors of verification technology and/or verified programs.

Finally, to avoid any misunderstanding as to our own views, let us make it clear that we in no way dispute that program verification can have a significant role to play in the vital task of clarifying specifications and removing design faults. That, however, is not the issue.

John Dobson and Brian Randell,
Computing Laboratory, University of Newcastle upon Tyne PHONE +44 91 222 7923

Computers in mathematical proof

Dale Worley <worley@compass.UUCP>
Thu, 22 Dec 88 10:43:19 EST

> From: Henry Cox <cox@spock.ee.mcgill.ca>
> Subject: Supercomputer used to "solve" math problem
>
> [Article about use of computer search to demonstrate the non-existence of a "projective plane of order 10 deleted. -- drw]
>
> 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

This is replaying a dispute that arose when the Four-Color Problem was solved

via computer search -- If no human mind has comprehended the proof, has it truly been proved? In the case of the Four-Color Problem, it is generally believed to be true, since other people (independently) wrote programs to check the solution.

However, from a broader perspective, this is ignoring the fact that many published mathematical proofs have significant errors in them, and not infrequently turn out to be "proving" entirely false statements. For instance there is a famous theorem whose proof was 300 pages long, in which 100 or so errors have been found (and corrected). Consider how many errors are probably in the proof of the Simple Group Theorem, which is a compendium of papers by 100 or so mathematicians, totalling about 2000 pages.

In cases not involving humans, no one would say "The willingness of people to accept other people's answers on faith remains disturbing" -- after all, we can't re-prove *everything* we read. When computers are involved, often the disturbing change is not that we take *more* on faith, but that it becomes *so obvious* we take things on faith.

Similarly, when a human controller screws up and causes a train collision, we consider this an unfortunate accident. When a computer control does the same, we wonder why people would rely on computers...

Personally, I'd rather depend on the cash register to do the addition than the minimum-wage clerk operating it.

Dale

Teaching students about responsible use of computers

Jerome H. Saltzer <Saltzer@ATHENA.MIT.EDU>
Thu, 22 Dec 88 15:51:46 EST

There has been some discussion in RISKS recently about what action universities might appropriately take to instill a sense of ethics in the use of computers by their students. M.I.T.'s Project Athena provides some 800 networked engineering workstations for undergraduates to use in any way they find helpful to their education. Accordingly, Project Athena has assumed that one of its responsibilities is to open a discussion of ethical use with its user community. The primary action that Project Athena has taken is the publication of a set of principles, a copy of the current version of which is attached.

These principles are for the most part general, following M.I.T.'s usual approach of appealing to basic concepts rather than spelling out many detailed rules. There is no claim that publicizing these principles completely solves any problem nor that it completely answers any question, but it does represent one organization's attempt to take a step in the right direction. Some version of these principles has been posted for about four years, and whenever we have an incident serious enough to ask a student to talk to the Director, these principles have provided a very useful starting point for the conversation.

Jerry Saltzer

----- ----- ----- ----- ----- ----- ----- ----- ----- ----- -----

Principles Of Responsible Use Of Project Athena

Project Athena is M.I.T.'s computing facility for education. It consists of a networked system of workstations and services, and includes communication features that offer many opportunities for members of the M.I.T. community to share information. With that ability to share comes the responsibility to use the system in accordance with M.I.T.'s standards of honesty and personal conduct. Those standards, outlined in the M.I.T. Bulletin under Academic Procedures, call for all members of the community to act in a responsible, ethical, and professional way. This note offers guidelines in applying those standards to use of Project Athena facilities.

INTENDED USE

The hardware granted to Project Athena, and the software licensed for that hardware, are intended for educational use, broadly construed, by members of the M.I.T. community. Use of Athena resources by anyone outside M.I.T. requires approval of the Provost, and the sale of such use is improper. The use of Athena resources for immediate financial gain is similarly improper. Use of Project Athena's facilities for sponsored research activities that normally would make use of other M.I.T. facilities requires specific authorization of the Director.

PRIVACY AND SECURITY

The operating systems used by Project Athena encourage sharing of information. Security mechanisms for protecting information from unintended access, from within the system or from the outside, are minimal. These mechanisms, by themselves, are not sufficient for a large community in which protection of individual privacy is as important as sharing. Users must supplement the system's security mechanisms by using the system in a manner that preserves the privacy of others.

For example, users should not attempt to gain access to the files or directories of another user without clear authorization from the other user (typically that authorization is expressed by setting file access permissions to allow public or group reading). Nor should users attempt to intercept any network communications, such as electronic mail or user-to-user dialog. A shared program should not secretly collect information about its users. Personal information about individuals, which a user would not normally disseminate, should not be stored or communicated on the system. Examples of such personal information are grades or letters of recommendation.

SYSTEM INTEGRITY

Actions taken by users intentionally to interfere with or to alter the integrity of the system are out of bounds. Such actions include unauthorized use of accounts, impersonation of other individuals in communications, attempts to capture or crack passwords or encryption, and destruction or alteration of data or programs belonging to other users. Equally unacceptable are intentional efforts to restrict or deny access by legitimate users to the system.

INTELLECTUAL PROPERTY RIGHTS

Some software and data that reside on the system are owned by users or third parties, and are protected by copyright and other laws, together with licenses and other contractual agreements. Users must abide by these restrictions. Such restrictions may include prohibitions against copying programs or data for use on non-Athena systems or for distribution outside M.I.T., against the resale of data or programs or the use of them for noneducational purposes or for financial gain, and against public disclosure of information about programs (e.g., source code) without the owner's authorization. It is the responsibility of the owner of protected software or data to make any such restrictions known to the user.

Responsible use of computers

Peter Neumann <neumann@csl.sri.com>
Thu, 22 Dec 1988 16:01:42 PST

There are still many would-be contributions in the RISKS pipeline on the general topic of computer misuse. Some reiterate points already made several times before. Others elaborate on relatively minor points. Thus, I have been a more rigorous enforcer of the RISKS guidelines than usual on this topic -- hopefully without unbalancing the representativity of the dialogue. I am grateful to Jerry for providing a general, principled view of part of the problem.

The bottom line is that responsibility is of necessity widely distributed. We certainly need better ethics and better laws, and better teaching of their implications. We also need a society that respects them. But our society needs much more that that; those of us who look at the world only from the vantage point of our computers are missing much. (I say this not just in the spirit of the season.)

Unfortunately, reality suggests that even the best ethics and laws will be violated by people responding to misplaced incentives (financial or otherwise). (The drug situation and insider trading are two examples that are difficult to combat with ethics and laws alone. They are deep social problems. And hacking can certainly become a social disease!) Thus, we also need computer systems that can enforce security and integrity much more thoroughly, and we need those systems to be administered and used intelligently. (That already may be expecting too much.) But by now it is generally realized that we cannot depend only on computer security controls -- there are just too many ways to break them in the systems that we must use.

So, to end the soap-box for this year, security, integrity, software safety and system safety (e.g., in the sense of Nancy Leveson, Avra Cohn, and others) are system-wide (and network-wide) concepts. There are many life-critical or other critical applications in which we must rely on both people and technology (especially computers) to perform properly (i.e., within tolerances); as we have seen in many cases discussed in RISKS, deviations may result in catastrophes that are unacceptable to the affected

individuals, if not to society as a whole. This applies to disastrous design flaws, programming errors, acts of God, and many other problems in addition to intentional system misuse. One rotten apple (human or technological) can spoil the barrel. The message for RISKS readers is once again that we must never blindly trust that computers and people will always do the right thing, and that we must plan accordingly. The problems require a comprehensive approach. If the real risks (as opposed to the perceived risks) are too great, then we had better rethink the use of computers in those applications. But let's honestly address the REAL RISKS.

Happy holidays! Peter

Search RISKS using swish-e

Report problems with the web pages to the maintainer